Appunti Algebra I

Questo documento contiene degli appunti presi durante il corso di algebra I (primo modulo). Mi auguro che possano essere utili a qualcuno.

Marco Centin, città degli studi di Milano Bicocca, luglio 2007.

Indice

1 Relazioni, funzioni, operazioni

1.1 Relazioni e funzioni

Definizione 1.1 *Siano X e Y insiemi non vuoti.*
Una relazione tra X e Y è un sottoinsieme del prodotto cartesiano $X \times Y$.
Se $R \subseteq X \times Y$ è una relazione e $x \in X,\ y \in Y$ sono due elementi tale che $(x, y) \in R$ si usa scrivere xRy e si dice che "x è in relazione con y".

Definizione 1.2 *Siano $X,\ Y,\ V$ insiemi non vuoti. Siano $R \subseteq X \times Y$ e $S \subseteq Y \times V$ due relazioni binarie. Si definisce prodotto o composizione [1] delle relazioni S ed R la relazione*

$$S \circ R := \{(x, v) \in X \times V :\ \exists y \in Y :\ (x, y) \in R\ \ e\ (y, v) \in S\}$$

La composizione di relazioni è associativa, cioè se $R \subseteq X \times Y$, $S \subseteq Y \times V$, $T \subseteq V \times W$ sono tre relazioni allora $T \circ (S \circ R) = (T \circ S) \circ R$.
La composizione non è in generale commutativa.

La definizione qui sopra si può interpretare dicendo che due elementi $x \in X$ e $v \in V$ sono in relazione tramite $S \circ R$ se esiste un elemento intermedio $y \in Y$ tale che x sia in relazione con y tramite R e y sia in relazione con v tramite S. Si noti che nella definizione la scrittura $R \circ S$ ha senso soltanto se $V = X$. Anche ponendo $X = Y = V$ in generale la composizione di relazioni non è commutativa.

Definizione 1.3 *Siano X e Y insiemi non vuoti.*
Una funzione (o applicazione, o mappa) da X a Y è una relazione $F \subseteq X \times Y$ tale che:

$$\forall x \in X\ \exists!\ y \in Y :\ (x, y) \in F$$

Se F è una funzione si scrive allora $F : X \to Y$ per indicare che è una funzione da X a Y. Se $(x, y) \in F$ si scrive $y = F(x)$ intendendo con tale scrittura che $y \in Y$ è quell'unico valore tale che $(x, y) \in F$. In modo analogo è possibile usare la seguente notazione:

$$x \overset{F}{\longmapsto} y$$

Dicendo che la funzione F mappa l'elemento $x \in X$ nell'elemento $y \in Y$ tale che $y = F(x)$. Si definiscono inoltre i seguenti insiemi:
$\forall A \subseteq X,\ A \neq \emptyset,\ F(A) := \{y \in Y :\ \exists x \in A :\ y = F(x)\}$
$\forall B \subseteq Y,\ B \neq \emptyset,\ F^{-1}(B) := \{x \in X :\ \exists y \in B :\ F(x) = y\}$
$F(\emptyset) := \emptyset; \qquad F^{-1}(\emptyset) := \emptyset$
$\forall y \in Y\ F^{-1}(y) := F^{-1}(\{y\})$
$\mathrm{im}F := F(X)$
Si noti che $F^{-1}(B)$ può essere vuoto. L'insieme $F(A)$ è detto immagine di A tramite F. L'insieme $F^{-1}(B)$ è detto controimmagine di B tramite F.

Definizione 1.4 *Siano $X,\ Y,\ Z$ tre insiemi non vuoti.*
Siano $f : X \to Y$ e $g : y \to Z$ due funzioni.
La composizione di f e g è la funzione

$$g \circ f : X \to Z \qquad x \longmapsto g(f(x))$$

[1] Nell'ordine assegnato.

La composizione di funzioni è associativa.
Cioè se $f : X \to Y$, $g : Y \to Z$, $h : Z \to T$ sono tre funzioni si ha:

$$h \circ g \circ f := (h \circ g) \circ f = h \circ (g \circ f)$$

Definizione 1.5 *Sia $f : X \to Y$ una funzione. Si dice che f è:*
(i) *Iniettiva se $\forall x_1, x_2 \in X : \ x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.*
(ii) *Suriettiva (o surgettiva, o surjettiva) se $f(X) = Y$.*
(iii) *Biettiva (o bigettiva, o bjettiva) se è suriettiva ed inettiva.*

OSSERVAZIONE Si noti che la condizione di iniettività di una funzione può essere espressa in una forma equivalente dalla proposizione contronominale. Cioè una funzione è iniettiva se e solo se:

$$\forall x_1, x_2 \in X : \ f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

Se X è un insieme non vuoto è possibile definire una funzione su X facendo corrispondere ogni elemento a se stesso. Cioè considerando la relazione formata da tutte le coppie $(x, x) : \ x \in X$. Tale applicazione viene detta relazione, applicazione o mappa identica e si denota con il simbolo id_X o semplicemente con I. In notazione funzionale id_X è quella funzione $f : \ \forall x \in x : \ f(x) = x$.

Definizione 1.6 *Sia $f : X \to Y$ una funzione.*
Si dice inversa sinistra di f una funzione $g : Y \to X$ tale che:

$$g \circ f = \mathrm{id}_X$$

Se esiste una tale funzione g si dice che f ammette g come inversa sinistra.

L'esistenza di una inversa sinistra di una funzione è condizione necessaria e sufficiente per la sua iniettività.

Proposizione 1.1 *Sia $f : X \to Y$ una funzione.*
Allora f è iniettiva se e solo se ammette inversa sinistra.

***D**imostrazione.*
Sia f iniettiva. Sia $y \in \mathrm{im}f$. Allora esiste un unico $x \in X$ tale che $y = f(x)$.
Definiamo $g : Y \to X$ ponendo:

$$g(y) := \begin{cases} x \in X : \ f(x) = y & \text{Se } y \in \mathrm{im}f \\ x_0 \in X : \ x_0 \text{ arbitrario} & \text{Se } y \notin \mathrm{im}f \end{cases}$$

g è una funzione. Sia $x \in X$. Si ha:

$$x \overset{f}{\longmapsto} f(x) \in \mathrm{im}f \overset{g}{\longmapsto} x$$

Quindi $g \circ f = \mathrm{id}_X$.
Viceversa, sia g un'inversa sinistra di f. Siano $x_1, x_2 \in X$ tali che $f(x_1) = f(x_2)$. Allora:

$$x_1 = (g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2) = x_2$$

Perciò f è iniettiva. ■

Definizione 1.7 *Sia $f : X \to Y$ una funzione.*
Si dice inversa destra di f una funzione $g : Y \to X$ tale che:

$$f \circ g = \mathrm{id}_Y$$

Se esiste una tale funzione g si dice che f ammette g come inversa destra.

L'esistenza di una inversa destra di una funzione è condizione necessaria e sufficiente per la sua surjettività.

Proposizione 1.2 *Sia $f : X \to Y$ una funzione.*
Allora f è suriettiva se e solo se ammette inversa destra.

***D**imostrazione.* Sia f suriettiva. Allora $\forall y \in Y \ f^{-1}(y) \neq \emptyset$.
Per ogni $y \in Y$ fissiamo $x_y \in f^{-1}(y)$ e definiamo $g : Y \to X$ ponendo
$\forall y \in Y \ g(y) := x_y$. g è una funzione. Inoltre:

$$y \overset{g}{\longmapsto} x_y \in f^{-1}(y) \overset{f}{\longmapsto} f(x) = y$$

Viceversa, sia $g : Y \to X$ un'inversa destra di f. Per ogni $y \in Y$ si ha:

$$f(g(y)) = (f \circ g)(y) = y = g(y) \in f^{-1}(y)$$

E quindi f è surgettiva. ■

Corollario 1.3 *Sia $f : X \to Y$ una funzione.*
Allora f è biettiva se e solo se ammette inversa sinistra e inversa destra.
In tal caso le due inverse coincidono e si dice che f ammette inversa bilatera, o semplicemente che f ammette inversa.

***D**imostrazione.* La prima parte della dimostrazione è immediata conseguenza della definizione. Proviamo che le due inverse coincidono. Sia g un'inversa sinistra e h un'inversa destra. Si ha $g \circ f = \mathrm{id}_X$ e $f \circ h = \mathrm{id}_Y$. Allora:

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

■

1.2 Relazioni di equivalenza

Un tipo particolare di relazioni hanno un' importanza fondamentale in algebra. Cominciamo con una definizione.

Definizione 1.8 *Sia X un insieme non vuoto. Sia $R \subseteq X^2$ una relazione su X. Si dice che R è una relazione di equivalenza se valgono le seguenti proprietà:*
(i) $\forall a \in X : \ aRa$ *(Riflessività)*
(ii) $\forall a, b \in X : \ aRb \Rightarrow bRa$ *(Simmetria)*
(iii) $\forall a, b, c \in X : \ aRb, bRc \Rightarrow aRc$ *(Transitività)*

Definizione 1.9 *Sia X un insieme non vuoto. Sia $R \subseteq X^2$ una relazione di equivalenza. Sia $a \in X$. L' insieme:*

$$[\, a \,]_R := \{x \in X : \ xRa\}$$

si chiama classe di equivalenza di a (individuata da R).

Lemma 1.4 *Sia X un insieme non vuoto e R una relazione di equivalenza su X. Allora:*
(i) $\forall a \in X : \ a \in [\, a \,]_R$
(ii) $\forall a, b \in X : \ aRb \Rightarrow [\, a \,]_R = [\, b \,]_R$
(iii) $\forall a, b \in X : \ a \not R b \Rightarrow [\, a \,]_R \cap [\, b \,]_R = \emptyset$

***D**imostrazione.* (i) Ovvia. (ii) $\forall x : xRa$ *e* $aRb \Rightarrow \forall x : xRb \Rightarrow [\, a \,]_R \subseteq [\, b \,]_R$.
In modo analogo $[\, b \,]_R \subseteq [\, a \,]_R$. (iii) Supponiamo per assurdo $[\, a \,]_R \cap [\, b \,]_R \neq \emptyset$. Sia $x \in [\, a \,]_R \cap [\, b \,]_R$. Deve essere xRa e xRb. Per la simmetria si ha aRx. Per la transitività aRb. Assurdo. ■

Definizione 1.10 *Sia X un insieme non vuoto. Sia $\{A_i : i \in I\}$ una collezione di sottoinsiemi non vuoti di X. Tale collezione si dice partizione di X se e solo se ogni elemento di X appartiene ad uno ed uno solo degli A_i.*
Si dice allora che l'insieme X è l'unione disgiunta degli insiemi A_i e si scrive:

$$X = \dot{\bigcup_{i \in I}} A_i$$

Proposizione 1.5 *Ogni relazione di equivalenza R su un insieme non vuoto X determina una partizione di X i cui elementi sono le classi $[\, a \,]_R$.*
Viceversa ogni partizione di un insieme non vuoto X determina una relazione di equivalenza le cui classi sono gli elementi della partizione.

***D**imostrazione.* Per il primo punto del lemma precedente ogni $x \in X$ appartiene ad una classe di equivalenza. Per il terzo punto tali classi sono disgiunte e sono quindi una partizione. Viceversa basta definire la relazione
$R : \forall a, b \in X : \ aRb \Leftrightarrow a, b \in A_i$ (sse appartengono allo stesso A_i). ■

Definizione 1.11 *Dato un insieme X non vuoto ed una relazione di equivalenza R si dice insieme quoziente di X rispetto alla relazione R l'insieme di tutte le classi di equivalenza e si indica con:*

$$X/R := \{\, [\, a \,]_R : \ a \in X \,\}$$

Definizione 1.12 *L'applicazione $\pi_R : X \to X/R$ che associa ad ogni elemento la sua classe di equivalenza:*

$$\forall a \in X, \;\; a \overset{\pi_R}{\longmapsto} [\, a \,]_R$$

Viene detta projezione naturale o canonica.

Come conseguenza immediata dell'ultima proposizione si ha che l'applicazione π_R è suriettiva. Allora, per quanto visto, π_R ammette un'inversa destra
$s : X/R \to X$ definita da:

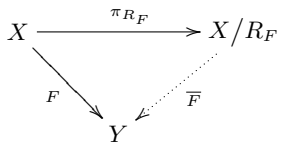
$$[\, x \,]_R \overset{s}{\longmapsto} y : \; yRx$$

L'insieme $R := \text{im}\; s \subseteq X$ si dice sistema di rappresentanti di R. Si noti che con la scrittura $[\, x \,]_R$ si denota la classe attraverso un suo rappresentante (non unico). Segue quindi che in generale $[\, a \,]_R = [\, b \,]_R$ non implica $a = b$.

Consideriamo ora un'applicazione $F : X \to Y$ possiamo definire una relazione di equivalenza R_F su X nel seguente modo:

$$\forall a, b \in X \;\; aR_F b \Leftrightarrow F(a) = F(b)$$

Cioè prendiamo tutte le coppie (a, b) per cui le immagini mediante F di a e b coincidono. Tale relazione è banalmente una relazione di equivalenza e viene detta *relazione di equivalenza associata ad F.*
Se si osserva il seguente diagramma commutativo[1]:



viene naturale chiedersi se possa esistere un'applicazione $\overline{F} : X/R_F \to Y$ che associ ad ogni classe di equivalenza un elemento $y \in Y$ in modo da poter "chiudere il diagramma, cioè in modo che $F \equiv \overline{F} \circ \pi_{R_F}$. Un altro modo di esprimere l'equazione $F = \overline{F} \circ \pi_{R_F}$ è dire che la funzione F *si fattorizza* mediante la proiezione canonica nel senso che verrà precisato più avanti reinterpretando la composizione $\circ$ come un'operazione.

Proviamo ora il fondamentale teorema d'omomorfismo per classi di insiemi.

[1] La commutatività del diagramma sarà conseguenza del teorema d'omomorfismo.

Teorema 1.6 (d'omomorfismo per classi di insiemi)
Siano X e Y insiemi non vuoti. Sia $F : X \to Y$ un'applicazione. Allora:
(i) *Esiste ed è unica un'applicazione $\overline{F} : X/R_F \to Y$ tale che*

$$F = \overline{F} \circ \pi_{R_F}$$

(ii) *$\overline{F}$ è iniettiva (sempre) ed è suriettiva (e quindi bjettiva) se e solo se F è suriettiva.*

***D**imostrazione.*
(i) Dimostriamo l'esistenza di $\overline{F}$. Definiamo $\overline{F} : X/R_F \to Y$ nel seguente modo:

$$[\,a\,]_{R_F} \overset{\overline{F}}{\longmapsto} F(a)$$

Si noti che a priori tale funzione non è ben definita in quanto se R è una generica relazione di equivalenza e $b \in [\,a\,]_R$ è un altro rappresentante della classe $[\,a\,]_R$ diverso da a allora l'applicazione $\overline{F}$ per definizione mappa la classe $[\,b\,]_R$ in $F(b)$ che, in generale, è diverso da $F(a)$. In questo caso però essendo $R = R_F$ si ha che:
$[\,a\,]_{R_F} = [\,b\,]_{R_F} \;\Rightarrow\; F(a) = F(b)$
e quindi $\overline{F}$ risulta una funzione ben definita.
Inoltre F si fattorizza mediante la projezione canonica in quanto:

$$(\overline{F} \circ \pi_{R_F})(a) = \overline{F}(\pi_{R_F}(a)) = \overline{F}([\,a\,]_{R_F}) = F(a)$$

Cioè $F = \overline{F} \circ \pi_{R_F}$. Proviamo l'unicità di $\overline{F}$.
Sia $\overline{F}'$ è un'altra applicazione tale che $F = \overline{F}' \circ \pi_{R_F}$. Allora:

$$\overline{F}'([\,a\,]_{R_F}) = F(a) = \overline{F}([\,a\,]_{R_F}) \;\Rightarrow\; \overline{F}' = \overline{F}$$

(ii) $\overline{F}$ è iniettiva. Infatti:

$$\overline{F}([\,a\,]_{R_F}) = \overline{F}([\,b\,]_{R_F}) \;\Rightarrow\; F(a) = F(b) \;\Rightarrow\; [\,a\,]_{R_F} = [\,b\,]_{R_F}$$

Infine $\overline{F}$ è suriettiva se e solo se F lo è perché:

$$\begin{aligned}\overline{F}(X/R_F) &= \{y \in Y : \exists a \in X :\; y = \overline{F}([\,a\,]_{R_F})\} = \\ &= \{y \in Y : \exists a \in X :\; y = F(a)\} = F(X)\end{aligned}$$

■

Osservazione Per la relazione R_F vale la seguente doppia implicazione:

$$[\,a\,]_{R_F} = [\,b\,]_{R_F} \Leftrightarrow F(a) = F(b)$$

Per dimostrare la prima parte dell'asserto si è fatto uso della sola implicazione:

$$[\,a\,]_{R_F} = [\,b\,]_{R_F} \Rightarrow F(a) = F(b)$$

Evidentemente quindi il punto (i) del teorema vale anche con una relazione X che soddisfi l'implicazione più debole. Per una tale X non sarà invece garantita la seconda parte del teorema.

1.3 Operazioni

Definizione 1.13 *Sia X un insieme non vuoto.*
Si dice operazione binaria definita su X ogni applicazione $* : X^2 \to X$
e si scrive:

$$(a, b) \overset{*}{\longmapsto} a * b$$

Così come si definisce un'operazione binaria è possibile definire un'operazione ternaria, quaternaria, n-aria. Se F è un'operazione n-aria si dice che F ha *arietà* n. In algebra hanno un'importanza fondamentale le operazioni binarie.

Definizione 1.14 *Sia $* : X^2 \to X$ un'operazione.*
(i) *$u_s \in X$ si dice unità sinistra per $*$ se $\forall x \in X\ u_s * x = x$.*
(ii) *$u_d \in X$ si dice unità destra per $*$ se $\forall x \in X\ x * u_d = x$.*
(iii) *$u \in X$ si dice unità (bilatera) per $*$ se $\forall x \in X\ u * x = x * u = x$.*

Proposizione 1.7 *Sia $* : X^2 \to X$ un'operazione.*
Se esistono una unità sinistra u_s e destra u_d per $*$, allora:
(i) *$u_s = u_d$*
(ii) *u_s è l'unica unità sinistra. u_d è l'unica unità destra.*
(iii) *Posto $u := u_s = u_d$, u è l'unica unità bilatera per $*$.*

***D**imostrazione.* (i) Siccome u_s è unità sinistra, $u_s * u_d = u_d$. Siccome u_d è unità destra $u_s * u_d = u_s$. (ii) Sia $\tilde{u}_s$ un'altra unità sinistra. Per il punto precedente $\tilde{u}_s = u_d = u_s$. (iii) Segue immediatamente da (i) e (ii). ∎

Definizione 1.15 *Sia $* : X^2 \to X$ un'operazione con unità u. Sia $x \in X$.*
(i) *Si dice che $\widehat{x}_s \in X$ è un inverso sinistro di x se $\widehat{x}_s * x = u$.*
(ii) *Si dice che $\widehat{x}_d \in X$ è un inverso destro di x se $x * \widehat{x}_d = u$.*
(iii) *Si dice che $\widehat{x} \in X$ è un inverso (bilatero) di x se $\widehat{x} * x = x * \widehat{x} = u$.*

Definizione 1.16 *Sia $* : X^2 \to X$ un'operazione.*
Si dice che $*$ è associativa se $\forall a,\ b,\ c \in X\ (a * b) * c = a * (b * c)$.

Proposizione 1.8 *Sia $* : X^2 \to X$ un'operazione associativa.*
Siano $a_1, \ldots, a_n \in X$. Allora $a_1 * \ldots * a_n$ non varia associando i termini in modi diversi[1]*.*

***D**imostrazione.* Procediamo per induzione su n. Per $n = 3$ è la proprietà associativa. Supponiamo la tesi vera per ogni $a_1, \ldots, a_n$ con $n <= n_0 - 1$. Allora possiamo porre $a := a_1 * \ldots * a_{n_0 - 1}$ per avere che $a_1 * \ldots * a_{n_0} = a * a_{n_0}$. E abbiamo finito. ∎

Definizione 1.17 *Sia $* : X^2 \to X$ un'operazione.*
Si dice che $*$ è commutativa se $\forall a,\ b \in X\ a * b = b * a$.

[1] Ma conservando l'ordine di $a_1, \ldots, a_n$!!!

Proposizione 1.9
Sia $* : X^2 \to X$ *un'operazione binaria associativa con unità* u*. Sia* $x \in X$*.*
Se esiste l'inverso sinistro $\widehat{x}_s$ *e l'inverso destro* $\widehat{x}_d$ *di* x *allora:*
(i) $\widehat{x}_s = \widehat{x}_d$
(ii) $\widehat{x} := \widehat{x}_s = \widehat{x}_d$ *è l'inverso bilatero di* x*.*
(iii) $\widehat{x}_s$*,* $\widehat{x}_d$ *e* $\widehat{x}$ *sono unici.*

D*imostrazione.* (i) Usando le proprietà dell'unità e quella associativa:
$\widehat{x}_s = \widehat{x}_s * u = \widehat{x}_s * (x * \widehat{x}_d) = (\widehat{x}_s * x) * \widehat{x}_d = u * \widehat{x}_d = \widehat{x}_d$
(ii) Ovvio. (iii) Sia $\widehat{x}'_s$ un altro inverso sinistro di x. Per il punto (i) deve essere $\widehat{x}'_s = \widehat{x}_d = \widehat{x}_s$. Discorso analogo per l'inverso destro. ■

Esempio Consideriamo un insieme non vuoto X e l'insieme $\mathcal{P}(X)$ delle parti di X. $\mathcal{P}(X)$ costituisce l'insieme di tutte le relazioni binarie su X. Se si considera la composizione di relazioni è evidente che $\circ$ è un'operazione sull'insieme $\mathcal{P}(X)$ in quanto manda ogni coppia di relazioni (X_1, X_2) in una ed una sola relazione $X_1 \circ X_2$. Tale operazione è associativa e ha come unità bilatera la relazione identica.
Infatti $\forall X \in \mathcal{P}(X)\ X \circ I = I \circ X = X$.

Definizione 1.18 *Sia* $* : X^2 \to X$ *un'operazione. Sia* $Y \subseteq X$ *non vuoto.*
Si dice che Y *è chiuso rispetto all'operazione* $*$ *se* $\forall y_1, y_2 \in Y\ y_1 * y_2 \in Y$*.*
Cioè se $*(Y^2) \subseteq Y$ *(se l'immagine di* $*$ *è contenuta in* Y*).*
Se Y *è chiuso rispetto a* $*$ *si può allora considerare la restrizione di* $*$ *a* Y *definita da:*

$$*_{/_Y} : Y^2 \to Y : \quad \forall y_1, y_2 \in Y \ \ y_1 *_{/_Y} y_2 := y_1 * y_2$$

Detto in altri termini la restrizione di un'operazione $*$ su Y è l'operazione $*_{/_Y}$ che agisce in Y esattamente come farebbe $*$.
Introduciamo ora un po' di notazione.

Notazione
Se X e Y sono insiemi non vuoti è possibile considerare l'insieme di tutte le applicazioni da $F : X \to Y$. Tale insieme si denota comunemente con il simbolo:

$$Y^X := \{F : X \to Y\}$$

Notazione che rivela la sua potenza in determinate situazioni. Consideriamo a titolo di esempio un sottoinsieme $X \subset \mathbb{N}$, $X := \{1, 2, \ldots, n\}$. Allora ogni funzione $F : X \to Y$ dove Y è un qualsiasi insieme finito. Allora è chiaro che l'insieme Y^X è in corrispondenza biunivoca con l'insieme delle n-uple ordinate di Y, che si indica con $Y^n = Y^{|X|}$.
L'insieme delle applicazioni $F : X \to X$, che è un sottoinsieme dell'insieme delle relazioni binarie su X, cioè consideriamo l'insieme $X^X \subseteq \mathcal{P}(X^2)$.
Chiaramente la composizione di funzioni da X a X è una funzione da X a X. Si ha quindi che X^X è chiuso rispetto a $\circ$.
Si noti X^X ha come unità bilatera la mappa identica id_X e che dato un elemento $F \in X^X$ l'inverso destro, sinistro e bilatero è esattamente l'inversa sinistra, destra o bilatera della funzione F secondo le definizioni precedenti.

OSSERVAZIONE Si mette in evidenza che alcune propietà di un dato insieme X sono state definite in termini di esistenza o meno di elementi in X con determinate proprietà. Altre invece sono state definite da un'equazione. Per questo motivo vengono dette *proprietà equazionali*. In questo capitolo si sono viste ad esempio la proprietà commutativa e quella associativa.
Se si considera la restrizione di un'operazione $*$ ad un insieme Y è evidente che le proprietà che in X erano espresse in termini equazionali continueranno valere in Y, mentre non sarà ovviamente garantita l'esistenza di elemento neutro o inverso perché tali elementi potrebbero appartenere a $X \setminus Y$.

OSSERVAZIONE Sia X non vuoto e sia $|X| = n$. $X = \{x_1, \ldots, x_n\}$.
Allora data un'operazione $* : X^2 \to X$ è possibile costruire una tabella a doppia entrata, detta *tavola di composizione*, dalla quale è possibile leggere alcune proprietà dell'operazione $*$. Costruendo la seguente tabella si avrà che:

$*$	x_1	x_2	$\cdots$	x_j	$\cdots$	x_n
x_1						
x_2						
$\vdots$						
x_i				$(x_i * x_j)$		
$\vdots$						
x_n						

- L'operazione è commutativa se e solo se la tavola di composizione è simmetrica rispetto alla diagonale principale.
- L'elemento $x_{\overline{i}}$ è unità sinistra se e solo se la $\overline{i}$-esima riga della tabella contiene $x_1, \ldots, x_n$. L'elemento $x_{\overline{j}}$ è unità destra se e solo se la $\overline{j}$-esima colonna della tabella contiene $x_1, \ldots, x_n$. Se $u := \overline{i} = \overline{j}$ allora x_u è l'unità bilatera.
- Se c'è l'unità bilatera x_u per trovare l'inverso sinistro di un x_j (se esiste) scorriamo la colonna relativa a x_j finchè non incontriamo x_u. Analogamente se esiste l'inverso destro di un x_i troveremo nella riga relativa a x_i l'unità x_u.

Un altro importante concetto è quello di operazione esterna.

Definizione 1.19 *Siano E ed X due insiemi non vuoti.*
Un'operazione esterna è una funzione da $E \times X$ in X definita da

$$(e, x) \longmapsto ex$$

In tal caso si dice allora che X è un E-insieme o che E opera su X.

1.4 Congruenze, relazioni compatibili

Tra le varie relazioni di equivalenza che si possono definire su una struttura algebrica quelle che rivestono maggior interesse sono quelle compatibili con le operazioni, nel senso che verrà precisato fra breve. Tali relazioni vengono anche dette congruenze.

Definizione 1.20 *Sia X un insieme su cui è definita un'operazione binaria $*$ e una relazione d'equivalenza R. Si dice che R è compatibile con l'operazione $*$, o che R è una congruenza rispetto all'operazione $*$, se $\forall a, a', b, b' \in X$*

$$aRa',\ bRb' \implies (a * b)R(a' * b')$$

Proposizione 1.10 *Sia X non vuoto. Sia $*$ un'operazione binaria su X.*
Sia R una relazione di equivalenza su X. Se[1] *R è una congruenza rispetto a $*$, allora è definita su X/R l'operazione $*_R : X/R \times X/R \to X/R$ ponendo $\forall\ [a]_R, [b]_R \in X/R$:*

$$[a]_R *_R [b]_R := [a * b]_R$$

***D**imostrazione.* Dimostriamo che tale operazione è ben definita. Ancora una volta a priori se $a' \in [a]_R$ ma $a' \neq a$ e $b' \in [b]_R$ ma $b' \neq b$ la funzione $*_R$ manda la coppia di classi $([a']_R, [b']_R)$ nella classe $[a' * b']_R$ che in generale è diversa da $[a * b]_R$. L'uguaglianza di queste due classi è garantita dall'ipotesi di compatibilità della relazione R con l'operazione $*$. ∎

Osservazione L'espressione che definisce l'operazione $*_R$ può essere letta anche nel seguente modo, attraverso la proiezione canonica:

$$\pi_R(a) *_R \pi_R(a) = \pi_R(a * b)$$

Con questa formulazione si dice che la proiezione canonica conserva il prodotto o analogamente che è un *morfismo* rispetto a $*$, termine che sarà chiaro più avanti.

[1] Se e solo se, in realtà.

2 Numeri interi

Sia $\mathbb{Z} = \{0,\ +1,\ -1,\ +2,\ -2,\ \dots\}$ l'insieme dei numeri interi con le operazioni di somma e moltiplicazione tradizionali.

2.1 Congruenze modulo n in $\mathbb{Z}$

$\mathbb{N} := \{1,\ 2,\ \dots\}$, $\mathbb{Z}_0 := \{0,\ 1,\ 2,\ \dots\}$. Le congruenze di numeri interi è il contesto originario in cui è nato il concetto di congruenza di una relazione rispetto ad un'operazione.

Teorema 2.1 (Divisione con resto) *Siano $n, m \in \mathbb{Z},\ m \neq 0$.*
Allora $\exists!\ q, r \in \mathbb{Z}$:
1) $n = mq + r$
2) $0 \leq r < |m|$

Definizione 2.1 *Siano $a,\ b \in \mathbb{Z}$.*
Si dice che b divide a e si scrive $b \mid a$ se $\exists\, c \in \mathbb{Z} :\ a = b \cdot c$.

Osservazione Si osservi ogni numero divide sempre se stesso: $\forall a \in \mathbb{Z}\ a \mid a$; se un numero a divide b e b divide c, allora anche a divide c. La relazione individuata dalla nozione di "dividere" è quindi riflessiva e transitiva; non è però una relazione simmetrica perché non è vero che se a divide b allora b divide a. Non è antisimmetrica perché se a divide b, b è diviso sia da a che da $-a$. Se restringessimo tale nozione all'insieme dei numeri naturali sarebbe antisimmetrica, e quindi una relazione d'ordine.

Definizione 2.2 *Sia $n \in \mathbb{Z},\ n > 1$.*
Se $a,\ b \in \mathbb{Z}$ diciamo che a è congruo a b modulo n e scriviamo

$$a \equiv b \ _{(n)}$$

Se $n \mid (a - b)$. Cioè se $\exists\, h \in \mathbb{Z}$ tale che $a - b = hn$.

Teorema 2.2 (Piccolo teorema di Fermat) [1]
Sia p un numero primo e $a \in \mathbb{Z} :\ \mathrm{MCD}(a, p) = 1$.
Allora $a^{p-1} \equiv 1 \ _{(p)}$

Ad esempio $100 \equiv 0 \ _{(2)}$, $50 \not\equiv 0 \ _{(4)}$, $9 \equiv 2 \ _{(7)}$, $3 \equiv -1 \ _{(4)}$, $2^6 \equiv 1 \ _{(7)}$, $2^{12} \equiv 1 \ _{(13)}$.

Proposizione 2.3
$\forall\, n > 1$ la relazione di congruenza modulo n è di equivalenza.
Le partizioni determinate dalle classi di quivalenza sono esattamente n.
Indicata con $[\,a\,]_n$ la classe di equivalenza contenente a, l'insieme delle classi di equivalenza fissato n sono $[\,0\,]_n,\ [\,1\,]_n,\ \dots, [\,n-1\,]_n$; sono cioè rappresentate da tutti i possibili resti nella divisione intera per n.

***D**imostrazione.* Proviamo che è una relazione di equivalenza.
Per prima cosa è riflessiva. Infatti ponendo $h = 0 \in \mathbb{Z}$, si ha:
$a - a = 0 \cdot n \implies a \equiv a \ _{(n)}$. Dimostriamo la simmetria.
Supponiamo che $a \equiv b \ _{(n)}$. Allora $\exists h \in \mathbb{Z} :\ a - b = hn$.
Ma allora: $b - a = (-h)n \implies b \equiv a \ _{(n)}$.

[1] Si veda la sottosezione successiva per una definizione di MCD.

Proviamo la transitività. Sia $a \equiv b \ _{(n)}$ e $b \equiv c \ _{(n)}$.
Allora $\exists h, k \in \mathbb{Z}$ tale che $a - b = hn$ e $b - c = kn$. Sommando membro a membro[2] otteniamo $a - c = (h + k)n$. Essendo $(h + k) \in \mathbb{Z}$ si ha che $a \equiv c \ _{(n)}$.
Proviamo ora che le classi di equivalenza sono tutte e sole le classi dei possibili resti della divisione per n. Sia $a \in \mathbb{Z}$. Consideriamo la classe $[\, a \,]_n$. Per il teorema della divisione con resto esistono q ed r, con $0 \leq r < n$, tali che $a = nq + r$.
Segue che $a - r = nq \implies a \equiv r \ _{(n)}$.
Quindi $[\, a \,]_n = [\, r \,]_n$, cioè la classe di a è la classe del suo resto r quando lo si divide per n. Allora le classi di equivalenza sono al più pari al numero dei possibili resti nella divisione per n, cioè n. Per provare che sono esattamente n si deve provare che classi corrispondenti a resti distinti sono distinte.
Siano allora i, j due possibili resti distinti ($0 \leq i,\ j < n$, con $i \neq j$).
Supponiamo per assurdo che sia $[\, i \,]_n = [\, j \,]_n$. Allora dovrebbe esistere un $h \in \mathbb{Z}$ tale che $i - j = hn$. Essendo però $0 \leq i,\ j < n$ la loro differenza non può essere un multiplo di n. Quindi deve essere $h = 0 \implies i - j = 0 \cdot n \implies i = j$, assurdo. ∎

Quindi data sull'insieme $\mathbb{Z}$ la relazione $\equiv_n$ di congruenza modulo n si ottiene una partizione i cui elementi sono le classi $[\, 0 \,]_n, \ldots, [\, n - 1 \,]_n$. La classe $[\, 0 \,]_n$ adesempio conterrà tutti i numeri interi divisibili per n, la classe $[\, 1 \,]_n$ (se esiste) conterrà i numeri interi della forma $1 + kn$ con $k \in \mathbb{Z}$ ... la classe k-esima (se esiste) conterrà gli elementi $x \in \mathbb{Z}$ tali che $x \equiv k \ _{(n)}$, da cui $x - k = hn$. Cioè conterrà gli elementi della forma $x = k + hn$.

Definizione 2.3 *Sia $\mathbb{Z}$ con la relazione $\equiv_n$ di congruenza modulo n.*
Allora le classi $[\, a \,]_n$ vengono dette classi resto e l'insieme quoziente viene indicato con

$$\mathbb{Z}/n\mathbb{Z} := \ \mathbb{Z}/ \equiv_n = \{[\, 0 \,]_n, \ldots, [\, n - 1 \,]_n\}$$

Mostriamo ora che la *congruenza modulo n* è una *congruenza* rispetto alle operazioni di somma e prodotto.

Proposizione 2.4
La congruenza modulo n è compatibile con $+$ e $\cdot$ definiti in $\mathbb{Z}$.

***D**imostrazione.*
Per provare la compatibilità con la somma dobbiamo provare che

$$a \equiv a' \ _{(n)},\ b \equiv b' \ _{(n)} \implies (a + b) \equiv (a' + b') \ _{(n)}$$

Le prime due condizioni implicano che esistono $h, k \in \mathbb{Z}$ tali che:
$a - a' = hn$ e $b - b' = kn$. Da queste ricaviamo $a = a' + hn$ e $b = b' + kn$.
Quindi $a + b = a' + hn + b' + kn = (a' + b') + (h + k)n$.
Essendo $h + k \in \mathbb{Z}$ segue che $(a + b) \equiv (a' + b') \ _{(n)}$.
Analogamente per il prodotto dobbiamo dimostrare che

$$a \equiv a' \ _{(n)},\ b \equiv b' \ _{(n)} \implies (ab) \equiv (a'b') \ _{(n)}$$

Ancora una volta si ha $a = a' + hn$ e $b = b' + kn$.
Allora $ab = (a' + hn)(b' + kn) = a'b' + (a'k + hb' + hkn)n$.
Siccome $(a'k + hb' + hkn) \in \mathbb{Z}$ si ha che $(ab) \equiv (a'b') \ _{(n)}$. ∎

[2] Cioè le proprietà delle operazioni $+$ e $\cdot$ in $\mathbb{Z}$.

Quindi per quanto visto è possibile definire sull'insieme $\mathbb{Z}/n\mathbb{Z}$ delle operazioni indotte dalla somma e dal prodotto di numeri relativi. Useremo per comodità ancora i simboli $+$ e $\cdot$ per denotare tali operazioni. La somma sarà definita da:

$$[\,a\,]_n + [\,b\,]_n := [\,a+b\,]_n$$

Tale operazione avrà come unità bilatera $[\,0\,]_n$ in quanto:

$$[\,a\,]_n + [\,0\,]_n = [\,a+0\,]_n = [\,a\,]_n = [\,0+a\,]_n = [\,0\,]_n + [\,a\,]_n$$

Inoltre la somma delle classi per come è stata definita eredita tutte le proprietà equazionali della somma sui numeri interi ed è quindi associativa e commutativa. È possibile inoltre definire un prodotto in $\mathbb{Z}/n\mathbb{Z}$ ponendo:

$$[\,a\,]_n \cdot [\,b\,]_n := [\,ab\,]_n$$

Per il prodotto l'unità bilatera sarà $[\,1\,]_n$. Infatti:

$$[\,a\,]_n \cdot [\,1\,]_n = [\,a \cdot 1\,]_n = [\,a\,]_n = [\,1 \cdot a\,]_n = [\,1\,]_n \cdot [\,a\,]_n$$

Esempio Poniamo $n = 6$ e scriviamo le tavole di composizione della somma e del prodotto in $\mathbb{Z}/6\mathbb{Z}$. Per comodità di scrittura si scriverà $\mathbf{k}$ invece di $[\,k\,]_6$, il lettore presti attenzione a questo particolare in modo da non confondere $[\,k\,]_6$ con il valore k.

$+$	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	**3**	**4**	**5**	**0**
2	**2**	**3**	**4**	**5**	**0**	**1**
3	**3**	**4**	**5**	**0**	**1**	**2**
4	**4**	**5**	**0**	**1**	**2**	**3**
5	**5**	**0**	**1**	**2**	**3**	**4**

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**
2	**0**	**2**	**4**	**0**	**2**	**4**
3	**0**	**3**	**0**	**3**	**0**	**3**
4	**0**	**4**	**2**	**0**	**4**	**2**
5	**0**	**5**	**4**	**3**	**2**	**1**

Dalla tavola di composizione della somma si può trovare l'inverso di un elemento di $\mathbb{Z}/6\mathbb{Z}$ semplicemente scorrendo la riga e cercando l'unità (cioè lo **0**). Ad esempio si ha che $\mathbf{4} + \mathbf{2} = \mathbf{0}$ ($[\,4\,]_6 + [\,2\,]_6 = [\,0\,]_6$) e quindi **4** è inverso sinistro (e bilatero, per la commutatività) di **2**. Osservando la tavola di composizione del prodotto si nota facilmente che non tutti gli elementi hanno inverso! Infatti non in tutte le righe e colonne compare l'unità del prodotto. Se si osserva attentamente quali elementi hanno un inverso si scopre che solo **1** e **5** hanno inverso (bilatero). È interessante notare che tali elementi sono gli unici *coprimi* con il valore 6. Sono gli unici x tale che $\mathrm{MCD}(x, 6) = 1$. Questa caratteristica in realtà vale in generale.

Siano $a, b \in \mathbb{Z}$. Una *congruenza lineare* modulo n è un'equazione della forma $ax \equiv b\ _{(n)}$ di cui si cerca la soluzione $x \in \mathbb{Z}$. Un risultato importante nella risoluzione di congruenze lineari è il seguente[3].

[3]La dimostrazione di questa proposizione verrà data nella prossima sottosezione.

Proposizione 2.5 *Sia $ax \equiv b \ _{(n)}$ una congruenza lineare modulo n. Allora tale congruenza ha soluzioni se e solo se* $\mathrm{MCD}(a, n) \mid b$.

Osservazione Sfruttando allora questo risultato possiamo mostrare che quanto affermato riguardo all'esistenza dell'inverso è vero. Infatti ponendo $b = 1$ la congruenza lineare diventa $ax \equiv 1 \ _{(n)}$ che, riletta sull'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$ tramite le operazioni indotte, diventa $[\,a\,]_n \cdot [\,x\,]_n = [\,1\,]_n$. Che è (per la commutatività) la condizione perché $[\,x\,]_n$ sia l'inverso bilatero di $[\,a\,]_n$. Ma allora l'enunciato del teorema afferma esattamente che esiste l'inverso se e solo se a ed n sono coprimi.

Esempio Se consideriamo la congruenza modulo 5 possiamo subito prevedere che ogni elemento non nullo di $\mathbb{Z}/5\mathbb{Z}$ ammette inverso rispetto al prodotto in tale insieme. Infatti le tavole di composizione su $\mathbb{Z}/5\mathbb{Z}$ sono:

$+$	**0**	**1**	**2**	**3**	**4**
0	**0**	**1**	**2**	**3**	**4**
1	**1**	**2**	**3**	**4**	**0**
2	**2**	**3**	**4**	**0**	**1**
3	**3**	**4**	**0**	**1**	**2**
4	**4**	**0**	**1**	**2**	**3**

$\cdot$	**0**	**1**	**2**	**3**	**4**
0	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**
2	**0**	**2**	**4**	**1**	**3**
3	**0**	**3**	**1**	**4**	**2**
4	**0**	**4**	**3**	**2**	**1**

E questa volta in ogni riga e colonna (**0** escluso) compare un **1**, come previsto. Inoltre l'insieme così costruito eredita da $\mathbb{Z}$ tutte le proprietà e in definitiva è possibile verificare che $(\mathbb{Z}/5\mathbb{Z}, +, \cdot)$ è un *campo*. Tale struttura ci fornisce allora uno strumento per la risoluzione di congruenze lineari.

Si dice *equazione diofantea* di primo grado un'equazione della forma $ax + by = c$, da risolvere in $\mathbb{Z}$. Supponiamo per esempio di dover risolvere l'equazione $2x - 5y = 3$. Possiamo riscrivere allora l'equazione come $2x-3 = y\cdot 5$, che equivale a dire $5 \mid (2x-3)$, che avviene se $2x \equiv 3 \ _{(5)}$. Passando allora da $\mathbb{Z}$ a $\mathbb{Z}/5\mathbb{Z}$ possiamo risolvere l'equazione con quanto visto [4]:

$$[\,2x\,]_5 = [\,3\,]_5 \ \Rightarrow \ [\,2\,]_5 \cdot [\,x\,]_5 = [\,3\,]_5 \ \Rightarrow \ ([\,3\,]_5 \cdot [\,2\,]_5) \cdot [\,x\,]_5 = [\,3\,]_5 \cdot [\,3\,]_5 \ \Rightarrow$$
$$\Rightarrow \ [\,x\,]_5 = [\,4\,]_5$$

Cioè le soluzioni sono della forma $x = 4 + 5k$ al variare di $k \in \mathbb{Z}$.
Introduciamo ora la nozione di massimo comun divisore.

[4] Il trucco consiste nel moltiplicare il tutto per un opportuno inverso (letto dalla tavola di composizione) in modo da isolare l'incognita. In questo caso l'inverso di **2** è **3**. Si noti però che perché tale inverso esista sempre in $\mathbb{Z}/n\mathbb{Z}$, n deve essere un numero primo.

2.2 Massimo comun divisore in $\mathbb{Z}$

Definizione 2.4 *Siano $a, b \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.*
Si dice massimo comun divisore tra a e b un qualsiasi numero $d \in \mathbb{Z}$ tale che:
(i) $d \mid a$ e $d \mid b$. *(d divide entrambi)*
(ii) *Se $c \mid a$ e $c \mid b$ allora $c \mid d$. (d è il massimo)*
Tale numero di viene denotato con il simbolo $\mathrm{MCD}(a, b) := d$.

Osservazione Si noti che se a e b sono interi non nulli e d è un loro massimo comun divisore anche $-d$ lo è. Se invece a e b sono positivi allora d è univocamente determinato, come mostra il seguente

Teorema 2.6 (Identità di Bézout)
Siano $a, b \in \mathbb{Z}^+$. Allora esiste $d \in \mathbb{Z}:$ $\mathrm{MCD}(a, b)$.
Tale numero d si può scrivere[5] *come combinazione lineare a coefficienti interi dei numeri a e b. Esistono cioè x e y in $\mathbb{Z}$ tali che:*

$$d = ax + by \qquad \textit{(Identità di Bézout)}$$

***D**imostrazione.* La dimostrazione è costruttiva e si basa sull'algoritmo delle divisioni successive enunciato nella sottosezione precedente. Siano dunque a e b positivi. Possiamo supporre $a > b$. Eseguendo le divisioni successive si ottiene:

1. $a = bq_1 + r_1$ con $0 \leq r_1 < b$
   Se $r_1 = 0$ si ha che $b \mid a$ e si termina.
   Se $r_1 \neq 0$ si prosegue dividendo b per r_1.
2. $b = r_1q_2 + r_2$ con $0 \leq r_2 < r_1$
   Se $r_2 = 0$ si ha che $r_1 \mid b$ (cha a sua volta divide a) e si termina.
   Se $r_2 \neq 0$ si prosegue dividendo r_1 per r_2.
3. $r_1 = r_2q_3 + r_3$ con $0 \leq r_3 < r_2$
   Se $r_3 = 0$ si ha che $r_2 \mid r_1$ e si termina.
   Se $r_3 \neq 0$ si prosegue dividendo r_2 per r_3.

   ...

(k-1). $r_{k-3} = r_{k-2}q_{k-1} + \mathbf{r_{k-1}}$ con $0 \leq r_{k-1} < r_{k-2}$
   Penultima divisione per cui $r_{k-1} \neq 0$. Si divide r_{k-2} per r_{k-3}.

(k). $r_{k-2} = r_{k-1}q_k + r_k$ con $0 \leq r_k < r_{k-1}$
   Con $r_k = 0$.

L'algoritmo delle divisioni successive ha termine perché produce una sequenza strettamente decrescente di resti positivi e interi che non può essere infinita:
$0 = r_k < r_{k-1} < r_{k-2} < \ldots < r_3 < r_2 < r_1 < b \leq a$.
Proviamo che l'ultimo resto non nullo $\mathbf{r_{k-1}}$ è il massimo comun divisore di a e b.
(i) Dall'ultima divisione si legge che $r_{k-2} = r_{k-1}q_k$ cioè che $r_{k-1} \mid r_{k-2}$.
Dalla penultima divisione si legge che $r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}$.
Siccome r_{k-1} divide sia il primo che il secondo addendo divide la somma, cioè $r_{k-1} \mid r_{k-3}$.
Risalendo tutte le divisioni si arriva a concludere che r_{k-1} divide sia a che b.
(ii) Supponiamo che esista un $c \in \mathbb{Z}^+$ tale che $c \mid a$ e $c \mid b$ e mostriamo che $c \mid r_{k-1}$.
Dalla prima divisione si legge che $a = bq_1 + r_1 \Leftrightarrow a - bq_1 = r_1$.
Se c divide sia a che b divide la somma $a - bq_1$, e quindi divide r_1.

[5] E la dimostrazione del teorema fornisce una procedura efficiente per farlo.

Dalla seconda divisione leggiamo $b = r_1q_2 + r_2 \Leftrightarrow b - r_1q_2 = r_2$.
Siccome c divide sia b che r_1 divide anche la somma, cioè r_2.
Proseguendo fino al passo $(k-1)$-esimo si deduce che c divide r_{k-1}.
Quindi $\text{MCD}(a, b) = \mathbf{r_{k\text{-}1}}$ e allo stesso tempo si è provata l'*identità di Bézout*.
Infatti dalle espressioni ricavate si ottiene:
$r_1 = a - bq_1$
$r_2 = b - r_1q_2 = b - (a - bq_1)q_2 = a \cdot (-1) + b \cdot (1 + q_1q_2)$
$\dots$
$r_{k-1} = ax + by$
Dove $x, y \in \mathbb{Z}$ sono determinati sostituendo r_{k-2} in r_{k-1}. ■

Osservazione La dimostrazione del teorema 2.6 fornisce una procedura per calcolare il massimo comun divisore tra due numeri detta *algoritmo delle divisioni successive* che consiste nel fare la divisione tra il numero più grande e quello più piccolo e poi tra il quoziente e il resto e così via. L'ultimo resto non nullo è il massimo comun divisore. L'identità di Bézout si ottiene quindi agevolmente partendo dalla penultima divisione ricavando il resto e sostituendo di volta in volta le espressioni ottenute ricavando i resti dalle divisioni precedenti.

Esempio Supponiamo di voler calcolare $\text{MCD}(200, 114)$.
Facendo le divisioni successive si ottiene:
$200 = 114 \cdot 1 + 86$; $114 = 86 \cdot 1 + 28$; $86 = 28 \cdot 3 + \mathbf{2}$; $28 = 2 \cdot 14 + 0$.
Si ha quindi che $\text{MCD}(200, 114) = 2$.
Per calcolare l'identità di Bézout ricaviamo i resti e sostituiamo risalendo:
$2 = 86 - 28 \cdot 3 = 86 - (114 - 86) \cdot 3 = 86 \cdot 4 - 114 \cdot 3 = (200 - 114) \cdot 4 - 114 \cdot 3 = 200 \cdot 4 - 114 \cdot 7$.
E l'identità di Bézout è appunto $2 = 4 \cdot 200 - 7 \cdot 114 = 200 \cdot x + 114 \cdot y$.

Osservazione Verrà usato spesso nelle dimostrazioni successive il seguente fatto. Se a e b sono numeri interi positivi e d è il massimo comun divisore tra a e b, allora d divide sia a che b e quindi esistono $\widetilde{a}$ e $\widetilde{b}$ tali che sia $a = \widetilde{a}d$ e $b = \widetilde{b}d$. Inoltre tali $\widetilde{a}$ e $\widetilde{b}$ hanno la caratteristica di essere coprimi in quanto, se così non fosse, avrebbero un fattore c in comune e quindi d non sarebbe il massimo comun divisore.

Lemma 2.7 $\text{MCD}(a + kn,\, n) = \text{MCD}(a,\, n)$

***D**imostrazione.* Sia $d := \text{MCD}(a, n)$ e sia $\overline{d} := \text{MCD}(a + kn,\, n)$.
Allora $d \mid n \implies d \mid kn$. Essendo inoltre $d \mid a$ si ha che $d \mid (a + kn) \implies d \mid \overline{d}$.
D'altra parte $\overline{d} \mid d$ in quanto $\overline{d} \mid kn$ e $d \mid a$. Infatti $\overline{d} \mid n \implies \overline{d}m = n$ e $\overline{d} \mid a + kn \implies \overline{d}h = a + kn$. Quindi si ottiene che $\overline{d}(h - km) = a$, cioè che $d \mid a$. Ma allora $d = \overline{d}$. ■

2.3 Congruenze linerari in $\mathbb{Z}$

Definizione 2.5 *Una congruenza lineare modulo n è un'equazione della forma $ax \equiv b \ _{(n)}$ di cui si cercano soluzioni $x \in \mathbb{Z}$.*

Proposizione 2.8 *Sia $ax \equiv b \ _{(n)}$ una congruenza lineare modulo n.*
Allora valgono le seguenti proprietà:
(i) $a \equiv b \ _{(n)} \implies a + c \equiv b + c \ _{(n)}$.
(ii) $a \equiv b \ _{(n)} \implies a \cdot c \equiv b \cdot c \ _{(n)}$.
(iii) $ca \equiv cb \ _{(n)} \implies a \equiv b \ _{(n/d)}$ *con* $d = \text{MCD}(c, n)$.

***D**imostrazione.*
(i) Supponendo che $a - b = kn$ si ha $\forall c \in \mathbb{Z}\ (a + c) - (b + c) = a - b = kn$.
(ii) In modo analogo si ha $ca - cb = c(a - b) = c(kn) = (ck)n$.
(iii) Essedo $d = \text{MCD}(c, n)$ si ha $c = \widetilde{c}d$ e $n = \widetilde{n}d$ per opportuni $\widetilde{c}, \widetilde{n} \in \mathbb{Z}$ con $\text{MCD}(\widetilde{c}, \widetilde{n}) = 1$. Allora da $ca - cb = kn$ segue che:

$$c(a - b) = kn \implies \widetilde{c}d(a - b) = \widetilde{n}dk \implies \widetilde{c}(a - b) = k\widetilde{n}$$

Ed essendo $\widetilde{c}$ ed $\widetilde{n}$ coprimi si ha che $\widetilde{c} \mid k$, cioè $k = s\widetilde{c}$ per un opportuno $s \in \mathbb{Z}$. Quindi:

$$\widetilde{c}(a - b) = k\widetilde{n} \implies \widetilde{c}(a - b) = s\widetilde{c}\widetilde{n} \implies a - b = s\widetilde{n} \implies a \equiv b \ _{(\widetilde{n})}$$

E questo conclude la dimostrazione. ■

Vediamo ora, come anticipato, un criterio per stabilire in modo semplice se una congruenza lineare ammette soluzioni.

Teorema 2.9 (Congruenze lineari)
Sia $ax \equiv b \ _{(n)}$ una congruenza lineare modulo n.
(i) *La congruenza ammette soluzione se e solo se* $\text{MCD}(a, n) \mid b$.
(ii) *Se la congruenza ammette soluzioni sia $d = \text{MCD}(a, n)$ e sia $\widetilde{n}$ tale che $n = \widetilde{n}d$. Allora se $c \in \mathbb{Z}$ è una soluzione particolare le soluzioni sono tutti e soli gli interi della forma $c + k\widetilde{n}$ al variare di k in $\mathbb{Z}$.*
(iii) *Se la congruenza ammette soluzioni ha esattamente d soluzioni a due a due non congrue modulo n.*

***D**imostrazione.*
(i) Supponiamo che la congruenza ammetta $c \in \mathbb{Z}$ come soluzione.
Sia $d = \text{MCD}(a, n)$. Si ha che d divide sia a che n.
Quindi $a = d\widetilde{a}$ e $n = d\widetilde{n}$ per qualche $\widetilde{a}$ e $\widetilde{n}$.
Siccome c è soluzione si ha $ac - b = hn$ per qualche $h \in \mathbb{Z}$. Allora:

$$ac - b = hn \implies (d\widetilde{a})c - b = h(d\widetilde{n}) \implies d(\widetilde{a}c - h\widetilde{n}) = b \implies d \mid b$$

Inversamente supponiamo che $d \mid b$. Allora $b = d\widetilde{b}$ con $\widetilde{b} \in \mathbb{Z}$.
Per l'identità di Bézout d si ha $d = sa + tn$ per opportuni s e t in $\mathbb{Z}$. Allora:

$$b = \widetilde{b}d = \widetilde{b}(sa + tn) = a(\widetilde{b}s) + n(\widetilde{b}t) \implies a(\widetilde{b}s) - b = n(-\widetilde{b}t)$$

Cioè esiste un $k = -\widetilde{b}t \in \mathbb{Z}$ tale che $a(\widetilde{b}s) - b = nk$, cioè $\widetilde{b}s$ è una soluzione dell'equazione. E il primo punto è così provato.

(ii) Supponiamo che c sia soluzione particolare e proviamo che $c + k\widetilde{n}$ è soluzione.
Ma infatti $d \mid a \;\Rightarrow\; a = \widetilde{a}d$ per un opportuno $\widetilde{a} \in \mathbb{Z}$. Da cui:

$$a(c + k\widetilde{n}) = ac + ak\widetilde{n} = ac + \widetilde{a}dk\widetilde{n} = ac + \widetilde{a}k(d\widetilde{n}) = ac + \widetilde{a}kn$$

Essendo c soluzione si ha $ac - b = hn \;\Rightarrow\; ac = b + hn$. Allora:

$$a(c + k\widetilde{n}) = ac + \widetilde{a}kn = (b + hn) + \widetilde{a}kn = b + (h + \widetilde{a}k)n$$

Cioè $c + k\widetilde{n}$ è soluzione. Come voluto.
Supponiamo viceversa che esista un'altra soluzione x e mostriamo che è della forma $c + k\widetilde{n}$. Dal fatto che x e c sono soluzioni segue che:

$$ax \equiv b \;_{(n)} \;\text{ e }\; ac \equiv b \;_{(n)} \;\Longrightarrow\; a(x - c) \equiv 0 \;_{(n)} \;\Longrightarrow\; a(x - c) = hn$$

Per un opportuno $h \in \mathbb{Z}$. Siccome d divide sia a che n si ha $a = \widetilde{a}d$ e $n = \widetilde{n}d$, per opportuni $\widetilde{a}$ e $\widetilde{n}$, coprimi tra loro. Allora segue che:

$$\widetilde{a}d(x - c) = h\widetilde{n}d \;\Rightarrow\; \widetilde{a}(x - c) = h\widetilde{n}$$

Siccome $\mathrm{MCD}(\widetilde{a}, \widetilde{n}) = 1$ segue che $\widetilde{a} \mid h$, ovvero $h = k\widetilde{a}$, $k \in \mathbb{Z}$. Allora:

$$\widetilde{a}(x - c) = k\widetilde{a}\widetilde{n} \;\Rightarrow\; x - c = k\widetilde{n} \;\Rightarrow\; x = c + k\widetilde{n}$$

(iii) Per il punto precedente le soluzioni sono c, $c+\widetilde{n}$, $c+2\widetilde{n}$, $\ldots$, $c+(d-1)\widetilde{n}$. Proviamo che sono a due a due non congrue. Siano per assurdo $c+r\widetilde{n}$ e $c+s\widetilde{n}$ con $0 \le r < s < d$ due soluzioni congrue modulo n. Allora:

$$c + s\widetilde{n} \equiv c + r\widetilde{n} \;_{(n)} \;\Longleftrightarrow\; s\widetilde{n} \equiv r\widetilde{n} \;_{(n)} \;\Longleftrightarrow\; s\widetilde{n} - r\widetilde{n} = kn$$

Per un opportuno $k \in \mathbb{Z}$. Allora, essendo $n = d\widetilde{n}$, si ha che:

$$\widetilde{n}(s - r) = k(d\widetilde{n}) \;\Longleftrightarrow\; s - r = kd \;\Longrightarrow\; d \mid s - r$$

Il che implica, essendo $s - r > 0$ che d sia minore di $s - r$.
Assurdo in quanto $0 \le r < s < d$. ■

Esempio Supponiamo di voler risolvere la congruenza:

$$64x \equiv 24 \;_{(20)}$$

Per prima cosa verifichiamo che ammetta soluzioni. Infatti $\mathrm{MCD}(64, 20) = 4$ e $4 \mid 24$. Possiamo quindi già concludere che la congruenza ammette esattamente 4 soluzioni non congrue a due a due. Calcoliamo ora le 4 soluzioni non congrue comprese tra 0 e il modulo 20 (tutte le altre saranno congrue a queste quattro).
Possiamo semplificare la congruenza notando che può essere scritta come:

$$4 \cdot 16x \equiv 4 \cdot 6 \;_{(4\cdot 5)} \;\Longrightarrow\; 16x \equiv 6 \;_{(5)}$$

Dove si è usata la proprietà (iii) della proposizione 2.8.
Adesso, come già osservato, dobbiamo trovare l'inverso di 16 in modo da moltiplicare a sinistra e avere scritto esplicitamente il valore della x. Esiste l'inverso?? Certamente! Infatti ora si ha $\mathrm{MCD}(16, 5) = 1$ e, per l'identità di Bézout, 1 può essere scritto come combinazione lineare di 15 e 5. Possiamo allora isolare il termine che moltiplica 5 ottenendo esattamente un numero congruo a 1 modulo 5 dall'altro lato.

Infatti dividendo 16 per 5 otteniamo: $16 = 3 \cdot 5 + 1 \implies 16 - 1 = 3 \cdot 5 \implies 16 \equiv 1 \ _{(5)}$. E quindi l'inverso cercato è 16. Moltiplicando per 16 e semplificando otteniamo quindi $x \equiv 96 \ _{(5)} \implies x \equiv 1 \ _{(5)}$. Quindi le soluzioni sono della forma $x = 1 + 5k$ al variare di k. In particolare i rappresentanti principali[6] sono $1, 6, 11, 16$.

OSSERVAZIONE Si noti che data una congruenza lineare $ax \equiv b \ _{(n)}$ se $\text{MCD}(a, n) = 1$ allora per l'identità di Bézout esiste l'inverso di a. Se invece $d = \text{MCD}(a, n) \neq 1$ allora potrebbe non esistere... ma se la congruenza ha soluzioni d divide b!! È allora possibile semplificare il fattore in comune usando le proprietà. A quel punto si ottiene una nuova congruenza dove si ha $\text{MCD}(a, n) = 1$ (come si è fatto nell'esempio).

[6] Si faccia attenzione al fatto che la congruenza che si deve risolvere è la prima! Le soluzioni devono essere a due a due non congrue modulo 20 (non modulo 5).

2.4 Numeri primi

Definizione 2.6 *Sia $p \in \mathbb{Z} \setminus \{0, 1, -1\}$. Si dice che:*
(i) *p è primo se ogni volta che p divide il prodotto di due numeri allora divide o uno o l'altro (o entrambi) cioè se è vera la seguente proposizione:*

$$\forall\, a, b \in \mathbb{Z} \qquad p \mid ab \implies p \mid a \ \vee\ p \mid b$$

(ii) *p è irriducibile se ammette come divisori solo $\pm p$ e ± 1. Cioè se vale la seguente:*

$$\forall\, n \in \mathbb{Z} \qquad n \mid p \implies n \in \{1, -1, p, -p\}$$

Osservazione Probabilmente il lettore conosce come definizione di numero primo la definizione di numero irriducibile. In effetti, come mostra la seguente proposizione, le due nozioni coincidono nel caso di numeri interi. Tuttavia il concetto di elemento primo ed elemento irriducibile possono essere estesi in altri contesti (come vedremo) in cui le due cose non sono equivalenti.

Proposizione 2.10 *Nell'insieme dei numeri interi $\mathbb{Z}$ (con la somma e il prodotto tradizionale) un numero $p \neq 0, \pm 1$ è primo se e solo se è irriducibile.*

***D**imostrazione.* Supponiamo $p \neq 0, \pm 1$ primo e proviamo che p è irriducibile. Supponiamo dunque che $n \mid p \implies p = n\widetilde{p}$ per qualche $\widetilde{p}$. Dal fatto che $p \mid p$ segue che $p \mid n\widetilde{p}$. Essendo p primo per ipotesi p divide n o p divide $\widetilde{p}$.
Nel primo caso $p \mid n$ (e $n \mid p$) $\implies n = \pm p$.
Nel secondo caso $p \mid \widetilde{p} \implies \widetilde{p} = ps \implies p = \widetilde{p}n = psn$ per qualche s. Ma allora $p(sn - 1) = 0$ ed essendo $p \neq 0$ per ipotesi deve essere $sn = 1 \implies n = s = \pm 1$ in quanto gli unici interi invertibili rispetto al prodotto sono ± 1.
Inversamente, supponiamo che $p \neq 0, \pm 1$ sia irriducibile e mostriamo che p è primo. Supponiamo che $p \mid mn$. Allora $mn = pq$ per qualche p, q. Sia $d := \mathrm{MCD}(p, n) \geq 0$ siccome $d \mid p$ e p è irriducibile o $d = 1$ oppure $d = |p|$.
Nel primo caso se $d = 1$ allora per l'identità di Bézout (teorema 2.6) esistono $x, y \in \mathbb{Z}$ tale che $1 = px + ny$. Ma allora si ha:

$$m = m \cdot 1 = m(px + ny) = pxm + \underbrace{nm}_{pq} y = p(\underbrace{xm + qy}_{\in \mathbb{Z}})$$

E quindi $p \mid m$. Nel secondo caso se $d = |p|$ allora $|p| \mid n \implies p \mid n$.
Dall'ipotesi $p \mid mn$ si ottiene quindi che $p \mid n$ o $p \mid n$ cioè p è primo. ∎

3 Strutture algebriche

Una struttura algebrica è nella sua forma più generale un insieme X non vuoto sul quale è definita una collezione $*_1, , \ldots, *_r$ di operazioni di arietà $n_1, \ldots, n_r$. Tra le strutture algebriche hanno però una importanza maggiore quelle binarie.

3.1 Semigruppi

Definizione 3.1 *Si dice semigruppo un insieme S non vuoto su cui è definita un'operazione binaria $*$ che goda della proprietà associativa.*
Un semigruppo si denota con la coppia $(S, *)$.

Esempi

1. $(\mathbb{N}, +)$ è un semigruppo in quanto la somma è associativa.
2. L'insieme $\{1, 2, 3, 4\}$ munito dell'operazione che associa a due numeri il minimo di essi è un semigruppo come è semplice verificare.
3. Tutti i monoidi e i gruppi delle definizioni seguenti sono in particolare anche dei semigruppi.

Osservazione
Esistono strutture algebriche in cui valgono condizioni più deboli della proprietà associativa. Se consideriamo due matrici $A, B \in \mathrm{Mat}(n, \mathbb{K})$ possiamo definire un prodotto $[,]$ nel seguente modo:

$$[A, B] := AB - BA$$

Tale prodotto è detto *prodotto di Lie* ed è anticommutativo in quanto $[A, B] = -[B, A]$. L'associatività in questo caso è sostituita dalla relazione

$$[[A, B], C] + [[B, C], A] + [[C, A], B] = 0$$

Chiamata *identità di Jacobe*, che può essere considerata una forma debole di proprietà associativa. Proseguiamo l'analisi nel caso in cui l'associatività vale.

3.2 Monoidi

Definizione 3.2 *Si dice monoide un semigruppo $(S, *)$ in cui l'operazione $*$ ammette unità bilatera. L'unità bilatera del monoide $(S, *)$ viene usualmente indicata con il simbolo 1_S. Se l'operazione è commutativa si dice che il monoide è commutativo o abeliano.*

Notazione
Ci sono due notazioni comunemente usate per queste strutture algebriche.
In *notazione moltiplicativa* l'operazione $*$ viene denotata con il simbolo di prodotto. Si scrive cioè ab o $a \cdot b$ invece di $a * b$. Con questa notazione l'unità si denota con il simbolo 1, o 1_S qualora si voglia specificare il gruppo.
In *notazione additiva* l'operazione $*$ viene denotata con il simbolo di somma. Si scrive cioè $a + b$ invece di $a * b$. Con questa notazione l'unità si denota con il simbolo 0, o 0_S qualora si voglia specificare il gruppo. In alcuni contesti l'unità in notazione additiva viene detta anche *zero*. Da qui in avanti si tenderà ad usare la notazione moltiplicativa. L'espressione "sia S un monoide" sarà solo l'abbreviazione di "sia $(S, \cdot)$ un monoide".

Esempi

1. $(\mathbb{Z}_0, +)$ è un monoide la cui unità è $u = 0$.
2. $(\mathbb{N}, \cdot)$ è un monoide la cui unità è $u = 1$.
3. $(\mathcal{P}(U), \cup)$ e $(\mathcal{P}(U), \cap)$ sono monoidi come pure $(\mathcal{P}(X^2), \circ)$. Le unità sono rispettivamente $\emptyset$, U e id.
4. Se $\mathrm{Mat}(n, \mathbb{K})$ è l'insieme delle matrici quadrate di ordine n sul campo $\mathbb{K}$ si ha che $(\mathrm{Mat}(n, \mathbb{K}), \cdot)$ (dove il prodotto è il classico prodotto di matrici riga per colonna) è un monoide non abeliano.

Definizione 3.3 *Sia $(S, *)$ un monoide.*
Un sottoinsieme $H \subseteq S$ si dice sottomonoide se valgono le seguenti:
(i) $1_S \in H$ *(l'unità sta in H)*
(ii) $\forall a, b \in H \; a * b \in H$ *(H è chiuso rispetto alla somma)*

Definizione 3.4 *Sia S un monoide. Sia $a \in S$. Sia $n \in \mathbb{Z}_0$.*
Si definisce potenza n-esima in base a l'elemento a^n definito da[1]*:*
1) $a^0 := 1_S$
2) $\forall n > 0 \; ; a^n := a^{n-1} \cdot a$

Proposizione 3.1 *Sia S un monoide.*
Per ogni $a \in S$ e $n, m \in \mathbb{Z}_0$ valgono le seguenti proprietà:
(i) $a^m \cdot a^n = a^{m+n}$
(ii) $(a^m)^n = a^{mn}$
Se il monoide è abeliano allora vale anche la seguente proprietà:
(iii) $\forall \, a, b \in S \;\; (ab)^n = a^n \cdot b^n$

***D**imostrazione.* (i) Sia m fissato. Procediamo per induzione su n.
Per $n = 0$ si ha $a^m a^0 = a^m 1_S = a^m = a^{m+0}$.
Supponiamo la tesi vera per $n - 1$ e mostriamola per n.
Per definizione di potenza e per ipotesi induttiva si ha:

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

(ii) Sia ancora m fissato e procediamo per induzione su n.
Per $n = 0$ si ha $(a^m)^0 = 1_S = a^0 = a^{m \cdot 0}$. Supponiamo la tesi vera per $n - 1$.
Per definizione di potenza e per il punto precedente si ha:

$$(a^m)^n = (a^m)^{n-1} \cdot (a^m) = a^{m(n-1)} \cdot a^m = a^{m(n-1)+m} = a^{mn}$$

(iii) Supponiamo quindi che S sia abeliano. Procediamo di nuovo per induzione.
Per $n = 0$ si ottiene $(ab)^0 = 1_S = 1_S \cdot 1_S = a^0 b^0$.
Ammessa vera per $n - 1$ si ottiene, usando la commutatività:

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

E questo conclude la dimostrazione. ∎

Osservazione
La definizione di potenza è una definizione ricorsiva che definisce una funzione potenza $\mathbb{Z}_0 \to S$ tale che dato un $a \in S$ ad ogni $n \in \mathbb{Z}_0$ associa l'elemento a^n.

[1] Si noti che nella definizione ricorsiva si è tenuto conto dell'ordine dei fattori $a_0, \ldots, a_n$.

Corollario 3.2 (e definizione) *Sia S un monoide e $a \in S$.*
L'insieme $\langle a \rangle := \{x \in S : \ x = a^n \ \text{ per qualche } n \geq 0\}$ è un sottomonoide detto sottomonoide ciclico generato da a.

***D**imostrazione.* Ovviamente l'insieme di tutte le potenze di un elemento contiene la potenza 0-esima che è l'unità. Se $x_1, x_2 \in \langle a \rangle$ allora $x_1 = a^m$ e $x_2 = a^n$ per opportuni m ed n. Allora $x_1 \cdot x_2 = a^{m+n} \in \langle a \rangle$. ■

Esempi

1. Nel monoide $(\mathbb{C}^*, \cdot)$ con $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Se ω è una radice primitiva n-esima di 1 allora $|\langle \omega \rangle| = n$.

3.3 Gruppi

Definizione 3.5 *Si dice gruppo un monode $(S, *)$ in cui ogni elemento di S ammette inverso bilatero. L'inverso bilatero di $x \in S$ viene usualmente indicato con il simbolo x^{-1}. Se l'operazione è commutativa si dice che il gruppo è commutativo o abeliano.*

Osservazione
Nella definizione di gruppo si è richiesto che l'operazione $*$ ammetta unità bilatera e che ogni elemento di S abbia inverso bilatero in S. In realtà sarebbe bastato definire un gruppo come un semigruppo in cui esiste l'unità sinistra per $*$ e l'inverso sinistro di ogni elemento. Infatti se $a \in S$ esiste l'inverso sinistro $b \in S$ di a, si ha cioè $ba = 1$. D'altra parte essendo $b \in S$ esiste anche l'inverso sinistro c di b, e quindi $cb = 1$. Essendo 1 l'unità sinistra si ha[2]:

$$ab = 1 \cdot (ab) = (cb) \cdot (ab) = c \cdot (ba) \cdot b = c \cdot (1 \cdot b) = cb = 1$$

Ponendo $a^{-1} := b$ si ha $a^{-1}a = aa^{-1} = 1$. Quindi aver ammesso l'esistenza di unità e inversi sinistri implica l'esistenza dell'inverso bilatero. Inoltre l'unità sinistra è anche unità destra (e quindi bilatera). Preso un $a \in S$ sia a^{-1} il suo inverso ($aa^{-1} = 1$). Siccome 1 è unità sinistra $\forall x \in S \ 1 \cdot x = x$. Allora si ha:

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

Cioè l'unità funziona anche da unità destra. Si osservi che in un gruppo, in forza delle proposizioni 1.7 e 1.9, l'unità e l'inverso di un dato elemento sono unici.

Esempi

1. $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ sono gruppi abeliani.
2. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sono gruppi abeliani.
3. L'insieme $\mathrm{GL}(n, \mathbb{R}) \subseteq \mathrm{Mat}(n, \mathbb{R})$ delle matrici non singolari, munito dell'operazione di prodotto di matrici è un gruppo non abeliano se $n > 1$.

Proposizione 3.3 *Sia G un gruppo.*
Allora valgono le seguenti proprietà:
(i) $\forall \ a, b \in G \ \ (ab)^{-1} = b^{-1}a^{-1}$ *(Regola del calzino).*
(ii) $\forall \ a, b, c \in G \ \ ab = ac \Rightarrow b = c \ \ e \ \ ba = ca \Rightarrow b = c$ *(Legge di cancellazione).*

[2] Usando due volte la proprietà associativa generalizzata.

***D**imostrazione.* (i) L'elemento $(ab)^{-1}$ è l'inverso di ab. Quindi $(ab)\cdot(ab)^{-1} = 1$. Essendo G un gruppo esiste a^{-1}. Moltiplicando a sinistra per a^{-1} si ottiene: $a^{-1}ab(ab)^{-1} = a^{-1}$ da cui $b(ab)^{-1} = a^{-1}$. Facendo la stessa cosa con b^{-1} si ha $b^{-1}b(ab)^{-1} = b^{-1}a^{-1}$, da cui l'asserto. (ii) Come già fatto due volte nel primo punto se $ab = ac$ basta moltiplicare a sinistra per a^{-1} e usare l'associatività. L'elemento a^{-1} esiste perché G è un gruppo. Se $ba = ca$ basta moltiplicare a destra per a^{-1}. ■

Osservazione Si osservi che perché valga la legge di cancellazione G deve essere un gruppo. La dimostrazione infatti usa ripetutamente la proprietà associativa e l'esistenza dell'inverso. Se consideriamo il monoide $(\mathrm{Mat}(n,\mathbb{K}),\cdot)$ la legge di cancellazione non vale in generale in quanto non tutte le matrici sono invertibili; infatti $(\mathrm{Mat}(n,\mathbb{K}),\cdot)$ non è un gruppo. Se $A, B, C \in \mathrm{Mat}(n,\mathbb{K})$ sono due matrici e si ha $AB = AC$ in generale non è possibile usare la legge di cancellazione e scrivere $B = C$. Se però $\det A \neq 0$ la matrice A è invertibile e si può "semplificare" A. Nel caso di $\mathbb{Z}$, che non è un gruppo rispetto a $\cdot$, la legge di cancellazione segue dalla regola di annullamento del prodotto: $ca = cb \Longrightarrow c(a-b) = 0 \Longrightarrow a - b = 0$ in quanto $c \neq 0$.

Definizione 3.6 *Sia G un gruppo. Sia $a \in G$. Sia $n \in \mathbb{Z}$.*
Si definisce potenza n-esima in base a l'elemento a^n definito da[3]*:*
1) $a^0 := 1_G$
2) *Se* $n > 0$ $a^n := a^{n-1}\cdot a$
3) *Se* $n < 0$ $a^n := (a^{-n})^{-1}$

Osservazione
Usando la notazione additiva la potenza viene detta *multiplo* e la definizione precedente si scrive nel seguente modo:
1') $0a := 0_G$
2') Se $n > 0$ $na := (n-1)a + a$
3') Se $n < 0$ $na := -((-n)a)$

Le proprietà delle potenze date per un monoide valgono nel caso dei gruppi anche con esponenti negativi e sono coerenti anche nel caso di esponente -1 e l'analogo teorema si dimostra con una semplice verifica.

Proposizione 3.4 *Sia S un gruppo.*
Per ogni $a \in S$ e $n, m \in \mathbb{Z}$ valgono le seguenti proprietà:
(i) $a^m \cdot a^n = a^{m+n}$
(ii) $(a^m)^n = a^{mn}$
Se il gruppo è abeliano proprietà:
(iii) $\forall\, a, b \in S$ $(ab)^n = a^n \cdot b^n$

[3]Si noti anche qui che nella definizione ricorsiva si è tenuto conto dell'ordine dei fattori $a_0, \ldots, a_n$ perché non è detto che il monoide sia abeliano.

3.4 Sottogruppi ciclici e ordine

Definizione 3.7 *Sia $(G, \cdot)$ un gruppo.*
Un sottoinsieme $H \subseteq G$ si dice sottogruppo se:
(i) $1_G \in H$ *(unità, e quindi $H \neq \emptyset$)*
(ii) $\forall a, b \in H \; ab \in H$ *(chiusura rispetto al prodotto)*
(iii) $\forall h \in H \; h^{-1} \in H$ *(chiusura rispetto all'inverso)*
Si scrive $H \leq G$ per indicare che H è un sottogruppo di G.

Si osservi che secondo la definizione data si ha subito che $(H, \cdot_{|H})$ è un gruppo.

Osservazione Se G è un gruppo esistono sempre almeno due sottogruppi. Infatti sia G che $\{1_G\}$ che soddisfano le condizioni richieste. Tali sottogruppi vengono detti *sottogruppi banali*. Ci si potrebbe chiedere quando un gruppo G ammette solo i sottogruppi banali. È possibile dimostrare che questo avviene quando G è finito e ha un numero primo di elementi.

Enunciamo e dimostriamo ora un utile criterio che è una condizione necessaria e sufficiente affinché un sottoinsieme H sia un sottogruppo di G.

Proposizione 3.5 (Criterio per sottogruppi qualsiasi)
Sia G un gruppo e $H \neq \emptyset$, $H \subseteq G$ un suo sottoinsieme.
Allora H è un sottogruppo di G se e solo se si verifica la seguente condizione:

$$\forall a, b \in H \quad ab^{-1} \in H$$

***D**imostrazione.* Ovviamente se H è un sottogruppo $\forall a, b \in H$, $b^{-1} \in H$ per la (iii), $ab^{-1} \in H$ per la (ii). Supponiamo viceversa vera la condizione del criterio.
(i) Per $a = b$ si ha $a \cdot a^{-1} \in H \implies 1_G \in H$.
(ii) Adesso che $1_G \in H$, per $a = 1_G$ si ha: $\forall\, b, \quad ab^{-1} = 1_G \cdot b^{-1} = b^{-1} \in H$.
(iii) Adesso che $\forall\, b$, $b^{-1} \in H$, per l'ipotesi $a(b^{-1})^{-1} = ab \in H$. ∎

Il seguente criterio è invece solo una condizione sufficiente che vale solo nel caso di sottogruppi con un numero finito di elementi.

Proposizione 3.6 (Criterio per sottogruppi finiti)
Sia G un gruppo e $H \neq \emptyset$, $H \subseteq G$ un suo sottoinsieme tale che $|H| = n < +\infty$.
Allora se H è chiuso rispetto al prodotto è un sottogruppo.

***D**imostrazione.* Essendo $H \neq \emptyset$, sia $a \in H$. Essendo H chiuso rispetto al prodotto tutte le potenze a^m stanno in H e prima o poi si ripetono in quanto H ha un numero finito di elementi. Quindi:

$$\exists\, r, s \in \mathbb{N}, \text{ con } r > s \text{ tale che } a^s = a^r$$

Essendo G un gruppo esiste $(a^r)^{-1} = a^{-r} \in G$ per cui, usando le proprietà (in G):

$$a^s = a^r \implies a^s a^{-r} = a^r a^{-r} \implies a^{s-r} = 1_G$$

Poniamo allora $t := s - r$. Se $t = 1$ allora $a^t = a = 1_G$.
Se $t > 1$ allora possiamo scrivere $a^t = a^{t-1} \cdot a = 1_G$.
Allora per l'unicità dell'inverso bilatero a^{t-1} è l'inverso di a, a^{-1}. Essendo una potenza di a, sta in H. Allora, essendo H chiuso rispetto al prodotto, si ha $aa^{-1} = 1_G \in H$. ∎

Lemma 3.7 *Sia G un gruppo e $\{H_i : i \in I\}$ una famiglia di sottogruppi. Allora $\bigcap_{i\in I} H_i$ è un sottogruppo di G.*

***D**imostrazione.*
(i) $\forall\, i \in I \;\; 1_G \in H_i \implies 1_G \in \bigcap_{i\in I} H_i$.
(ii) $\forall\, i \in I \;\; (a, b \in H_i \Rightarrow ab \in H_i) \implies (a, b \in \bigcap_{i\in I} H_i \Rightarrow ab \in \bigcap_{i\in I} H_i)$.
(iii) $\forall\, i \in I \;\; (h \in H_i \Rightarrow h^{-1} \in H_i) \implies (h \in \bigcap_{i\in I} H_i \Rightarrow h^{-1} \in \bigcap_{i\in I} H_i)$. ∎

Definizione 3.8 *Sia G un gruppo e $A \subseteq G$ un sottoinsieme non vuoto. Si definisce sottogruppo generato dall'insieme A l'intersezione di tutti i gruppi che contengono A. Tale insieme viene indicato con il simbolo $\langle A\rangle$. Se $A = \{\, a\}$ si usa scrivere $\langle a\rangle$ invece che $\langle\{\, a\}\rangle$. In tal caso si dice che $H = \langle a\rangle$ è il gruppo ciclico generato dall'elemento a.*

Lemma 3.8 *Ogni gruppo ciclico è abeliano.*

***D**imostrazione.* Sia G un gruppo ciclico e siano $a, b \in G$. Allora, essendo $G = \langle g\rangle$ ciclico, deve essere $a = g^n$ e $b = g^m$ per opportuni $n, m \in \mathbb{Z}$. Allora per 3.1 si ha:

$$ab = g^n g^m = g^{n+m} = g^{m+n} = g^m g^n = ba$$

Cioè G è abeliano. ∎

Proposizione 3.9 *Sia G un gruppo e A un sottoinsieme non vuoto di G. Allora $\langle A\rangle$ è costituito da tutti e soli gli elementi di G esprimibili come prodotto di un numero finito di elementi di A e di inversi di elementi di A. Cioè:*

$$\langle A\rangle = \left\{\, g \in G :\; g = \prod_{i=1}^{n} a_i^{\varepsilon_i} \;\; \textit{con } n \in \mathbb{N},\; a_i \in A,\; \varepsilon_i = \pm 1 \,\right\}$$

***D**imostrazione.* Chiamiamo X l'insieme considerato. Proviamo che è un gruppo.
(i) Sia $a \in A$. $a = \prod_{i=i}^{1} a^1 \implies a \in X$; $a^{-1} = \prod_{i=i}^{1} a^{-1} \implies a^{-1} \in X$.
Allora $\prod_{i=1}^{1} a^{\varepsilon_i} = a \cdot a^{-1} \in X$.
(ii) Sia $x \in X$. Allora x è della forma $x = \prod_{i=1}^{n} a_i^{\varepsilon_i}$. Si ha dunque:

$$x^{-1} = \left(\prod_{i=1}^{n} a_i^{\varepsilon_i}\right)^{-1} = \prod_{i=1}^{n} a_{n-i}^{\varepsilon_i} \in X$$

Dove l'ordine dei fattori è invertito in quanto non è detto che il gruppo G sia abeliano.
(iii) Se $a, b \in X$ allora:

$$a \cdot b = \left(\prod_{i=1}^{n} a_i^{\varepsilon_i}\right) \cdot \left(\prod_{i=1}^{m} b_i^{\varepsilon_i}\right) = a_1^{\varepsilon_{i_1}} \dots a_n^{\varepsilon_{i_n}} \cdot b_1^{\varepsilon_{i_1}} \dots b_m^{\varepsilon_{i_m}} = \prod_{j=1}^{n+m} c_j^{\beta_j}$$

E quindi $ab \in X$. Inoltre tale gruppo contiene banalmente A in quanto ogni elemento di A si può scrivere come produttoria di se stesso alla prima potenza. Dimostriamo che è il più piccolo gruppo contenente A. Supponiamo che H sia un sottogruppo tale che $A \subseteq H$ e mostriamo che $X \subseteq H$. Preso un $x \in X$ si ha $x = \prod_{i=1}^{n} a_i^{\varepsilon_i}$. Essendo H un gruppo contenente A deve contenere anche ogni inverso di A e tutte le potenze di A in quanto deve essere chiuso rispetto al prodotto e deve esistere l'inverso. Inoltre $1_G \in H$. Allora tutti gli $a_i^{\varepsilon_i}$ stanno anche in H e quindi $x \in H$. Quindi $\forall\, x \in X \; x \in H \implies X \subseteq H$. ∎

Definizione 3.9 *Sia G un gruppo e $a \in G$. Si definisce ordine o periodo del gruppo ciclico generato da a la quantità $|\langle a \rangle|$ e viene indicato con il simbolo $o(a)$.*

Proposizione 3.10
Sia G un gruppo ed $a \in G$ tale che $o(a) = n < +\infty$. Allora:
(i) *n è il minimo intero positivo tale che $a^n = 1_G$.*
(ii) *Gli elementi distinti di $\langle a \rangle$ sono $1_G = a^0, a^1, \ldots, a^{n-1}$.*
(iii) *$a^l = a^m \iff l \equiv m \ _{(n)}$.*
Inoltre $o(a) = +\infty$ se e solo se la funzione potenza è iniettiva.
Cioè se e solo se $l \neq m \implies a^l \neq a^m$.

***D**imostrazione.* (i) e (ii) Sia $n = o(a)$.
Essendo $o(a)$ finito le potenze di a non possono essere tutte distinte.
Siano allora $i, j \in \mathbb{Z}$ con $i > j$ i più piccoli esponenti per cui $a^i = a^j$.
Moltiplicando a sinistra per a^{-j} si ha $a^{i-j} = 1_G$.
Quindi esiste un minimo valore $t := i - j > 0$ per cui $a^t = 1_G$.
Ogni $h \in \mathbb{Z}$ può essere diviso per t. Quindi $\forall\, h \in \mathbb{Z} :\ h = qt + r \ \text{ con } \ 0 \leq r < t$.
Allora la generica potenza h-esima è

$$a^h = a^{qt+r} = (a^t)^q \cdot a^r = (1_G)^q \cdot a^r = 1_G \cdot a^r = a^r$$

uguale ad una potenza r-esima con $0 \leq r < t$. Quindi $n \leq t$.
Proviamo che $t \leq n$ mostrando che gli elementi dell'insieme: $I := \{a^0, \ldots, a^t\}$ sono tutti distinti. Siano per assurdo $a^{k_1}, a^{k_2} \in I$ $(0 \leq k_2 < k_1 < t)$ tali che $a^{k_1} = a^{k_2}$.
Allora si avrebbe $a^{k_1 - k_2} = 1_G$ con $k_1 - k_2 < t$, assurdo in quanto t è il mimino valore per cui questo avviene.
(iii) Sia ora $a^l = a^m$. Proviamo che $l \equiv m \ _{(n)}$.
Dividendo $l - m$ per n, e sfruttanto il punto precedente si ha:

$$a^l = a^m \implies 1_G = a^{l-m} = a^{nq+r} = (a^n)^q \cdot a^r = (1_G)^q \cdot a^r = a^r$$

Con $0 \leq r < n$. Per la minimalità di n deve essere necessariamente $r = 0$.
Allora $l - m = nq + 0 \implies l \equiv m \ _{(n)}$.
Inversamente si ha:

$$l \equiv m \ _{(n)} \implies l - m = hn \implies a^{l-m} = a^{hn} = (a^n)^h = 1_G \implies a^l = a^m$$

Infine il sottogruppo ciclico generato da a ha ordine infinito se e solo se la funzione potenza è iniettiva. Infatti se $l \neq m \implies a^l \neq a^m$ l'ordine è ovviamente non finito.
Viceversa se l'ordine è infinito supponiamo per assurdo $a^l = a^m$ con $l > m$.
Allora per il punto (i) si avrebbe:

$$a^l = a^m \implies a^{l-m} = 1_G \implies o(a) \leq l - m$$

E questo è assurdo in quanto per ipotesi $o(a) = \infty$. ∎

Osservazione Se G è un gruppo finito di ordine n sulla base di quanto appena visto si ha che dato un elemento $a \in G$ e un intero positivo k se $a^k = 1_G = a^0$ allora si può concludere che $k \equiv 0 \ _{(n)}$ cioè che esiste $h \in \mathbb{Z}^+$ tale che $k - 0 = hn$. Quindi se $a^k = 1_G$ si ha che $n \mid k$. In particolare $n \leq k$. Questo fatto verrà usato spesso nelle prossime dimostrazioni, assieme al fatto che se $d = \text{MCD}(k, n)$ allora, essendo d un divisore comune, esistono $\widetilde{k}$ ed $\widetilde{n}$ tali che $k = \widetilde{k}d$ e $n = \widetilde{n}d$.

Proposizione 3.11 *Sia G un gruppo ed $a \in G$. Allora:*
(i) $\forall\, a \in G:\ \ o(a) = o(a^{-1})$.
(ii) *Se $r \in \mathbb{Z}^*$ è tale che $a^r = 1_G$, allora* $o(a) \mid r$

***D**imostrazione.* (i) Sia $n = o(a)$. n è il minimo intero positivo tale che $a^n = 1_G$. Allora si ha che per tale valore anche $(a^{-1})^n = 1_G$ in quanto:

$$a^n = 1_G \implies (a^{-1})^n = (a^n)^{-1} = 1_G^{-1} = 1_G$$

Quindi $o(a^{-1}) \leq n$. Poniamo $m := o(a^{-1})$. Allora:

$$(a^{-1})^m = 1_G \implies (a^m)^{-1} = 1_G \implies a^m = ((a^m)^{-1})^{-1} = 1_G^{-1} = 1_G$$

Quindi $n = o(a) \leq m$. Allora non può che essere $m = n$.
(ii) Per il primo punto possiamo supporre $r > 0$. Poniamo $n := o(a)$ e dividiamo r per n ottenendo $r = nq + r_1$ con $0 \leq r_1 < n$. Allora:

$$1_G = a^r = a^{nq+r_1} = (a^n)^q \cdot a^{r_1} = (1_G)^q \cdot a^{r_1} = a^{r_1}$$

Per la minimalità di n, a^{r_1} può essere 1_G sse $r_1 = 0$.
Ma allora $r = nq + 0 \implies n \mid r$ ■

Proposizione 3.12 *Sia G un gruppo, sia $a \in G$. Allora:*
(i) *Se* $o(a) = \infty$ *allora* $\forall\, k \neq 0 \ \ o(a^k) = \infty$.
(ii) *Se* $o(a) = n < \infty$ *allora* $\forall\, k \neq 0 \ \ o(a^k) = n/\mathrm{MCD}(k, n)$.
(iii) *Se* $o(a) = n < \infty$ *allora* $\langle a \rangle = \langle a^k \rangle \iff \mathrm{MCD}(k, o(a)) = 1$

***D**imostrazione.* (i) Per 3.11 possiamo supporre $k > 0$. Supponiamo per assurdo che $o(a^k) = m < \infty$ allora per 3.10 si ha $1_G = (a^k)^m = a^{km}$ e quindi, sempre per 3.10, si avrebbe $o(a) \leq km$. Assurdo: $o(a) = \infty$.
(ii) Sia $n := o(a)$ e $d := \mathrm{MCD}(k, n)$. Anche qui possiamo supporre $k > 0$.
Siano $\widetilde{n}$ e $\widetilde{k}$ tali che $n = \widetilde{n}d$ e $k = \widetilde{k}d$. Allora:

$$(a^k)^{\widetilde{n}} = a^{k\widetilde{n}} = a^{\widetilde{k}d\widetilde{n}} = a^{\widetilde{k}n} = (a^n)^{\widetilde{k}} = (1_G)^{\widetilde{k}} = 1_G$$

Quindi, sulla base di quanto già osservato, $o(a^k) \mid \widetilde{n}$. Mostriamo che anche $\widetilde{n} \mid o(a^k)$ in modo da poter concludere (in quanto $k > 0$) che $o(a^k) = \widetilde{n}$.
Ma infatti, posto $t := o(a^k)$ si ha:

$$(a^k)^t = 1_G = a^{kt} \implies n \mid kt \implies \exists\, h \in \mathbb{Z}:\ nh = kt$$

Ma allora da $nh = kt$ segue $\widetilde{n}dh = \widetilde{k}dt \ \Rightarrow\ \widetilde{n} \mid \widetilde{k}t$. Essendo però $\mathrm{MCD}(\widetilde{n}, \widetilde{k}) = 1$ deve essere necessariamente $\widetilde{n} \mid t$, come voluto.
(iii) Sia $d := \mathrm{MCD}(k, n)$. Ovviamente se $\langle a \rangle = \langle a^k \rangle$ allora $n = o(a) = o(a^k) = n/d$ implica $d = 1$. Viceversa se $d = 1$ allora $o(a^k) = o(a)/d = o(a)$ e quindi $|\langle a^k \rangle| = |\langle a \rangle|$.
Per la proposizione 3.9 ogni potenza a^p sta in $|\langle a \rangle|$ e quindi $\langle a \rangle \subseteq \langle a^k \rangle$. L'uguaglianza segue dal fatto che i due insiemi sono finiti e hanno uguale cardinalità. ■

Esempi

1. $(\mathbb{Z}, +)$ è un gruppo ciclico generato da $+1$ oppure -1 in quanto ogni intero z può essere scritto come $z = 1 + 1 + \ldots + 1 = z \cdot 1 = (-z) \cdot (-1)$.

2. $(\mathbb{Z}/n\mathbb{Z}, +)$ è un gruppo ciclico generato da $[1]_n$.
   Infatti $[k]_n = [1]_n + \ldots + [1]_n = k\,[1]_n$ dove con $k\,[1]_n$ si intende la potenza k-esima di $[1]_n$ scritta in notazione additiva. Ci sono altri generatori?
   Essendo $[1]_n$ un generatore, se $[g]_n$ è un altro generatore lo si deve poter ottenere da un multiplo (potenza) di $[1]_n$. Quindi deve essere $[g]_n = k\,[1]_n$. Allora $[g]_n$ è un generatore se e solo se (per la proposizione 3.12):

   $$\langle [1]_n \rangle = \mathbb{Z}/n\mathbb{Z} = \langle [g]_n \rangle = \langle k\,[1]_n \rangle \iff \mathrm{MCD}(k, n) = 1$$

   Ad esempio $\mathbb{Z}/4\mathbb{Z}$ è generato da $[1]_4$ e $[3]_4$; $\mathbb{Z}/5\mathbb{Z}$ è generato da $[1]_5, [2]_5, [3]_5, [4]_5$.
   Se n è primo allora $\mathbb{Z}/n\mathbb{Z}$ è un gruppo ciclico generato da ogni suo elemento.
3. $(\mathbb{Q}, +)$ **non** è un gruppo ciclico in quanto dato un elemento $p/q \in \mathbb{Q}$, i multipli (potenze) di p/q sono gli elementi $h \cdot p/q$, e non tutti i numeri razionali si ottengono come multiplo di p/q.

Lemma 3.13 *Sia G un gruppo* abeliano.
Siano $x, y \in G$ tali che $\mathrm{MCD}(o(x), o(y)) = 1$. *Allora:*

$$o(xy) = o(x) \cdot o(y)$$

***D**imostrazione.* Sia $n := o(x)$, $m := o(y)$, $t := o(xy)$.
Allora, essendo G abeliano si ha: $(xy)^{nm} = (x^n)^m \cdot (y^m)^n = 1_G \cdot 1_G = 1_G$.
Segue che $t \mid mn$. Si ha inoltre $1_G = (xy)^t = x^t \cdot y^t \implies x^t = y^{-t} \implies x^t \in \langle x \rangle \cap \langle y \rangle$.
Ma l'intersezione $\langle x \rangle \cap \langle y \rangle$ contiene solo l'unità. Infatti sia $z \in \langle x \rangle \cap \langle y \rangle$. Allora $o(z) \mid n$ e $o(z) \mid m$. Segue che $o(z) \mid \mathrm{MCD}(m, n) = 1$. E l'elemento che ha ordine 1 è l'unità. Allora $x^t = 1_G \implies n \mid t$, $y^{-t} = 1_G \implies m \mid t$ e quindi, essendo m ed n coprimi si ha che $mn \mid t$. Si conclude che $mn = t$. ∎

3.5 Gruppi di permutazioni

Nel 1872 il matematico tedesco Felix Klein formulò un programma, conosciuto come Programma di Erlangen, in cui la geometria venne interpretata come studio delle proprietà dello spazio che sono invarianti rispetto a un dato gruppo di trasformazioni. Questo punto di vista unificante della geometria oggi è accettato come standard. Per questo motivo le trasformazioni giocano un ruolo maggiore nella matematica moderna.

Sia X un insieme non vuoto. Indichiamo con S_X l'insieme delle applicazioni bijettive di X in sé, dette anche *trasformazioni* su X (specialmente quando X è infinito). $(S_X, \circ)$ è un gruppo detto *gruppo simmetrico* su X. Se $|X| = n < \infty$ poniamo lo chiamiamo *gruppo di permutazioni* e lo indichiamo con il simbolo S_n o con la corrispondente lettera gotica $\mathfrak{S}_n$. Ovviamente si ha $|\mathfrak{S}_n| = n!$.

Una generica *permutazione* $\sigma \in S_n$ può essere scritta come segue:

$$\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} \qquad \text{ove} \quad b_i = \sigma(a_i)$$

Mettendo in evidenza le immagini dei singoli elementi a_i. Esistono delle permutazioni particolarmente semplici detti *cicli* di lunghezza $r \geq 2$ dati da:

$$c = \begin{pmatrix} c_1 & c_2 & \dots & c_r & c_{r+1} & \dots & c_n \\ c_2 & c_3 & \dots & c_1 & c_{r+1} & \dots & c_n \end{pmatrix}$$

Se $r = 2$ i cicli vengono detti *scambi*. Nel caso dei cicli si preferisce usare la seguente notazione, meno pesante:

$$c = (c_1\ c_2\ \dots\ c_r)$$

Intendendo in questo modo che l'elemento c_1 viene mappato nell'elemento c_2 che viene mappato in $c_3 \dots$ fino ad arrivare all'elemento c_r che viene mappato nell'elemento a_1. Tutti gli altri elementi vengono mandati in se stessi. Un ciclo di lunghezza r ammette quindi r scritture distinte.

Se $\sigma \in S_X$ è una permutazione si dice che σ *muove* a_i se $\sigma(a_i) \neq a_i$. Si dice che σ *fissa* a_i se $\sigma(a_i) = a_i$. Se $\sigma(a_i) = a_i$ si dice anche che a_i è un *punto fisso* per la permutazione σ. Nel caso dei cicli di lunghezza r, c muove tutti gli elementi a_i con $1 \leq i \leq r$ e fissa gli altri. La notazione introdotta per i cicli non è unica.
Tutte le seguenti scritture seguenti indicano lo stesso ciclo:

$$c = (c_1\ c_2\ \dots\ c_r) = (c_2\ c_3\ \dots\ c_r\ c_1) = \dots = (c_r\ c_1\ \dots\ c_{r-1})$$

Se $\sigma, \tau \in S_X$ sono due bijezioni di X in sé si dice che σ e τ sono *disgiunte* se gli elementi di X mossi da σ sono fissati da τ e viceversa.
In tal caso ovviamente il prodotto di σ e τ commuta: $\sigma \circ \tau = \tau \circ \sigma$.

Proposizione 3.14
Ogni permutazione $\sigma \in \mathfrak{S}_n$ è prodotto di un numero finito di cicli disgiunti univocamente determinati da σ a meno dell'ordine.

***D**imostrazione.* (intuitiva)
Ogni elemento a_i o è mosso o è fissato da σ. Partiamo da a_1.
Se a_1 è fissato da σ passiamo ad a_2. Se sono tutti fissati concludiamo che σ è l'applicazione identica. Altrimenti arriverà un a_k che è mosso da σ. L'elemento $a_t = \sigma(a_k)$ deve essere necessariamente mosso perché se fosse fissato avrebbe due preimmagini, contro la bijettività di σ. La stessa cose deve essere per $\sigma(a_t)$ e così via. Procedendo in questo modo per la bijettività di σ il cammino deve terminare necessariamente su a_k, concludendo un ciclo. Se nel cammino si sono percorsi tutti gli a_i si termina altrimenti si riparte da un qualsiasi punto non percorso. Alla fine si ottengono un numero finito di cicli disgiunti. Una formalizzazione più rigorosa di questa dimostrazione si può dare per induzione. ■

ESEMPIO Per $X = \{1, 2, \ldots, 10\}$ sia $\sigma \in \mathfrak{S}_{10}$ la permutazione definita da:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 5 & 4 & 1 & 6 & 10 & 9 & 8 & 7 \end{pmatrix}$$

Partendo ad esempio da 1 e seguendo la procedura usata nella dimostrazione si trovano facilmente i cicli disgiunti di cui σ è composta:

$$\sigma = (1\ 2\ 3\ 4\ 5) \circ (7\ 10) \circ (8\ 9)$$

Si usa spesso quando X è un insieme con un numero n di elementi identificare gli elementi di X con i primi n numeri naturali (nel seguito si darà per scontato questo fatto). Ad esempio S_1 è un gruppo banale dato dalla sola permutazione identica: $S_1 = \{\mathrm{id}_X\}$; $S_2 = \{\mathrm{id}_X, (1\ 2)\}$; $S_3 = \{\mathrm{id}_X, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$
E così via (S_4 ha 24 elementi). Si noti che S_1 ed S_2 sono gruppi abeliani. S_3 invece è il più piccolo esempio di gruppo non abeliano. Infatti:

$$(1\ 2) \circ (1\ 2\ 3) = (2\ 3) \neq (1\ 3) = (1\ 2\ 3) \circ (1\ 2)$$

Se $|X| = n$ e $Y \subseteq X$ è un suo sottoinsieme tale che $0 < |Y| < |X|$, allora l'insieme delle permutazioni di X che fissano tutti gli elementi di $X \setminus Y$ è identificabile (isomorfo) a S_Y. Quindi S_n con $n \geq 3$ non è un gruppo abeliano.

Definizione 3.10 *Sia $\sigma \in S_n$ una permutazione.*
Si definisce segno della permutazione σ la quantità:

$$\Delta\sigma := \prod_{1 \leq i < j \leq n} \frac{b_i - b_j}{a_i - a_j} = \pm 1 \quad \textit{dove} \quad \sigma = \begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$$

Se $\Delta\sigma = +1$ si dice che σ è pari. Se $\Delta\sigma = -1$ si dice che σ è dispari.

Si ponga l'attenzione sulla condizione $i < j$ nella produttoria. Il segno di una permutazione vale ± 1 in quanto, stando alla bijettività di σ, nel prodotto capita a denominatore la stessa quantità che capita che capita in un altro numeratore (eventualmente cambiata di segno).

Vediamo ora come il segno di una permutazione è legato alla composizione.

Proposizione 3.15 *Siano $\sigma, \tau \in S_n$ due permutazioni. Allora:*

$$\Delta(\tau \circ \sigma) = \Delta\tau \cdot \Delta\sigma$$

***D**imostrazione.*
Sia σ definita come sopra. Sia τ definita da:

$$\begin{pmatrix} b_1 & b_2 & \dots & b_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix} \quad \text{allora} \quad \tau \circ \sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ c_1 & c_2 & \dots & c_n \end{pmatrix}$$

Quindi si ha:

$$\Delta(\tau \circ \sigma) = \prod_{1 \le i < j \le n} \frac{c_i - c_j}{a_i - a_j}$$

D'altra parte

$$\Delta\tau \cdot \Delta\sigma = \left(\prod_{1 \le i < j \le n} \frac{c_i - c_j}{b_i - b_j} \right) \cdot \left(\prod_{1 \le i < j \le n} \frac{b_i - b_j}{a_i - a_j} \right) = \prod_{1 \le i < j \le n} \frac{c_i - c_j}{a_i - a_j}$$

Come risultato della semplifica delle quantità $b_i - b_j$ che copaiono sotto gli stessi indici da entrambe le parti. ■

La permutazione identica ha segno $+1$, qualsiasi scambio ha invece segno -1.
L'insieme delle permutazioni pari è un sottogruppo del gruppo simmetrico S_n, viene detto *gruppo alterno* e si indica con $\mathbb{A}_n$ o con la corrispondente lettera gotica $\mathfrak{A}_n$.
È un gruppo in quanto:
(i) $\mathrm{id} \in \mathbb{A}_n$ in quanto è pari.
(ii) Se $\sigma, \tau \in \mathbb{A}_n$ allora $\Delta(\tau \circ \sigma) = \Delta\tau \cdot \Delta\sigma = 1 \cdot 1 = 1$
(iii) Se $\sigma \in \mathbb{A}_n$ allora anche $\sigma^{-1} \in \mathbb{A}_n$ in quanto:

$$1 = \Delta(\mathrm{id}) = \Delta(\sigma \circ \sigma^{-1}) = \Delta(\sigma) \cdot \Delta(\sigma^{-1}) = 1 \cdot \Delta(\sigma^{-1}) = \Delta(\sigma^{-1})$$

Proposizione 3.16 *Sia C_r un ciclo di lunghezza r.*
Allora C_r può essere decomposto come prodotto di $r-1$ scambi:

$$C_r = (c_1,\, c_r) \circ (c_1,\, c_{r-1}) \circ \dots \circ (c_1,\, c_3) \circ (c_1,\, c_2)$$

In particolare un ciclo di lunghezza pari è una permutazione dispari.
Un ciclo di lunghezza dispari è una permutazione pari.

***D**imostrazione.* La prima parte vale per definizione di composizione. Per la seconda, essendo c_r dato dal prodotto di $r-1$ scambi, il suo segno è $(-1)^{r-1}$. ■

Proposizione 3.17 *Sia $\sigma \in \mathfrak{S}_n$ una permutazione.*
Sia $\sigma = C_{r_1} \circ \dots \circ C_{r_t}$ la sua decomposizione come prodotto di t cicli disgiunti di lunghezza $r_1, \dots r_t$. Allora il segno di σ è dato da:

$$\Delta(\sigma) = (-1)^{\beta} \quad \textit{con} \quad \beta = \left(\sum_{i=1}^{t} r_i \right) - t$$

***D**imostrazione.* σ può essere scomposta in un prodotto di t cicli disgiunti $C_{r_1}, \dots, C_{r_t}$ di lunghezze $r_1, \dots, r_t$ e di segno $(-1)^{r_1 - 1}, \dots, (-1)^{r_t - 1}$. Quindi il segno di σ è il prodotto di queste quantità. ■

4 Teoria elementare dei gruppi

Trattiamo ora con maggiore dettaglio alcuni risultati riguardo alla struttura di gruppo attraverso lo studio delle congruenze. Introdurremo il concetto di classi laterali, sottogruppi normali, morfismi e gruppi quoziente.

4.1 Classi laterali, teorema di Lagrange

Definizione 4.1 *Sia G un gruppo e H un suo sottogruppo.*
Definiamo le due relazioni D_H ed S_H come:
$D_H: \ \forall\, a, b \in G \quad aD_Hb \ \ sse \ \ \exists\, h \in H \ \ tale\ che \ \ b = ha.$
$S_H: \ \forall\, a, b \in G \quad aS_Hb \ \ sse \ \ \exists\, h \in H \ \ tale\ che \ \ b = ah.$

Lemma 4.1 *Le relazioni D_H ed S_H sono di equivalenza.*

***D**imostrazione.* Proviamo l'asserto per D_H. La dimostrazione per S_H è analoga.
(i) $\forall\, a \in G \ \ aD_Ha$ in quanto $a = 1_G \cdot a$, e $a \in H$.
(ii) $aD_Hb \implies \exists\, h \in H: \ \ b = ha \implies h^{-1}b = h^{-1}ha = a \implies bD_Ha$.
(iii) Se aD_Hb e bD_Hc allora da $b = h_1a$ e $c = h_2b$ segue $c = h_2(h_1a) = (h_1h_2)a$. ∎

Definizione 4.2 *Le classi di equivalenza di D_H si dicono laterali destri del sottogruppo H. Le classi di equivalenza di S_H si dicono laterali sinistri di H e si pone:*

$$Ha := [\,a\,]_{D_H} = \{g \in G: \ \exists\, h \in H: \ g = ha\}$$
$$aH := [\,a\,]_{S_H} = \{g \in G: \ \exists\, h \in H: \ g = ah\}$$

È possibile, laddove non ci siano possibilità di confusione, indicare con $H\backslash G$ l'insieme dei laterali destri e con G/H l'insieme dei laterali sinistri.

In notazione additiva i laterali destri e sinistri si indicano con $H + a$ e $a + H$. Si osservi che la cardinalità di un laterale è uguale a quella di H. Si sottolinea che dal fatto che $Ha = Hb$ **non** si deduce che $a = b$, ma una delle condizioni espresse nel seguente:

Lemma 4.2 *Sia G un gruppo e $H \leq G$ un suo sottogruppo.*
Siano aH e bH le classi laterali sinistre di H in G. Allora sono equivalenti:
(i) $aH = bH$
(ii) $aH \cap bH \neq \emptyset$
(iii) $a \in bH$
(iv) $b^{-1}a \in H$

***D**imostrazione.* (i)⇒(ii) Essendo H non vuoto si ha $aH \cap bH = aH \neq \emptyset$.
(ii)⇒(iii)⇔(iv) Sia $c \in aH \cap bH$. Allora $c = ah_1 = bh_2$ per opportuni h_1 ed h_2 in H. Moltiplicando prima a destra per h_1^{-1} e poi a sinistra per b si ottiene:

$$ah_1 = bh_2 \implies a = bh_2h_1^{-1} \ \ (\text{cioè } a \in bH) \iff b^{-1}a = h_2h_1^{-1} \ \ (\text{cioè } b^{-1}a \in H)$$

(iv)⇒(i) Sia $ah_1 \in aH$. Per la (iii), che è equivalente alla (iv), si ha $a \in bH$, e quindi $a = bh_2$. Da cui $ah_1 = bh_2h_1 \in bH$. Quindi $aH \subseteq bH$. Ora, se $b^{-1}a \in H$, allora anche il suo inverso $a^{-1}b$ sta in H. Quindi $a^{-1}b = h_1 \implies b = ah_1$. Allora se $bh_2 \in bH$ si ha $bh_2 = ah_1h_2 \in aH$, e quindi $bH \subseteq aH$. ∎

Proposizione 4.3 *Sia G un gruppo ed H un suo sottogruppo. Sia G/H l'insieme dei laterali sinistri e $H\backslash G$ l'insieme dei laterali destri di H in G. Allora la funzione $f : G/H \to H\backslash G$ definita da $f(gH) := Hg^{-1}$ è una bijezione tra l'insieme dei laterali sinistri e l'insieme dei laterali destri. In particolare $|G/H| = |H\backslash G|$.*

***D**imostrazione.* L'applicazione è ovviamente suriettiva ed è iniettiva in quanto dal fatto che $f(g_1H) = f(g_2H)$ segue $Hg_1^{-1} = Hg_2^{-1}$. Quindi per opportuni $h_1, h_2 \in H$ si ha $h_1g_1^{-1} = h_2g_2^{-1}$. Allora deve essere vero che $(h_1g_1^{-1})^{-1} = (h_2g_2^{-1})^{-1}$, cioè $g_1h_1^{-1} = g_2h_2^{-1}$. Ma essendo che $h_1^{-1}, h_2^{-1} \in H$ si ha che $g_1H = g_2H$. ∎

Definizione 4.3 *Dato un sottogruppo H del gruppo G si definisce indice di H e si denota con $(G : H)$ la cardinalità comune dell'insieme dei laterali destri e sinistri.*

Osservazione Le relazioni D_H ed S_H sono due relazioni differenti. Prendiamo ad esempio il gruppo $G = S_3 = \mathfrak{S}_3$ ed il sottogruppo $H = \langle(1\ 2)\rangle$ generato dallo scambio $(1\ 2)$. Allora la relazione D_H dà luogo alla partizione: $H1_G = H = \{\ \mathrm{id},\ (1\ 2)\}$ $H(1\ 3) = H = \{\ (1\ 3),\ (1\ 2) \circ (1\ 3) = (1\ 3\ 2)\}$ $H(2\ 3) = H = \{\ (2\ 3),\ (1\ 2) \circ (2\ 3) = (1\ 2\ 3)\}$ Invece S_H dà luogo alla partizione: $1_GH = H = \{\ \mathrm{id},\ (1\ 2)\}$ $(1\ 3)H = H = \{\ (1\ 3),\ (1\ 3) \circ (1\ 2) = (1\ 2\ 3)\}$ $(2\ 3)H = H = \{\ (2\ 3),\ (2\ 3) \circ (1\ 2) = (1\ 3\ 2)\}$ E questo basta a mostrare che in generale $D_H \neq S_H$.

Teorema 4.4 (Lagrange)
Sia G un gruppo finito di ordine n ed H un suo sottogruppo di ordine r.
Allora $r \mid n$, e il quoziente tra n ed r è il numero dei possibili laterali (indice di H).

***D**imostrazione.* Consideriamo la relazione D_H. Essa determina una partizione disgiunta formata da s classi distinte. Si ha cioè che: $G = Ha_1 \dot\cup Ha_2 \dot\cup \ldots \dot\cup Ha_s$.
La funzione che associa ad ogni $h \in H$ l'elemento ha è una bijezione fra H ed Ha.
Suriettiva in quanto ogni elemento di Ha si scrive, per definizione, della forma ha.
Iniettiva in quanto $h_1a = h_2a \Longrightarrow h_1 = h_2$. Quindi si ha che $\forall\, i = 1, \ldots, s\ |Ha_i| = |H|$.
Segue che:

$$n = |G| = |Ha_1| + |Ha_2| + \ldots + |Ha_s| = s \cdot |H| = sr$$

In particolare si ha quindi che $r \mid n$. ∎

Corollario 4.5 *Sia G un gruppo finito di ordine n. Sia $a \in G$.*
Allora $o(\langle a\rangle)$ è un divisore di n. In particolare $a^n = 1_G$.

Corollario 4.6 *Le seguenti affermazioni sono equivalenti:*
(i) *G è un gruppo ciclico di ordine primo.*
(ii) *G è un gruppo di ordine primo.*
(iii) *G ammette solo i due sottogruppi banali G e $\{\ 1_G\ \}$.*

***D**imostrazione.* (i)⇒(ii) Ovvio. (ii)⇒(iii) Per il teorema di Lagrange se $H \leq G$ allora o $|H| = 1$ oppure $|H| = |G|$. Ma tali sottogruppi sono solo quelli banali. (iii)⇒(i) Se G ammette i due distinti sottogruppi banali allora G non è banale. Sia dunque $g \in G,\ g \neq 1_G$ e consideriamo il sottogruppo $\langle g\rangle$. Per la (iii) deve essere $\langle g\rangle = G$. Quindi G è ciclico. Se G fosse infinito allora sarebbe isomorfo[1] a $\mathbb{Z}$ e quindi ammetterebbe infiniti sottogruppi. Quindi diciamo $|G| = n < \infty$. Per 3.12 si ha che se $n = ab$ allora

$$o(g^b) = \frac{n}{\mathrm{MCD}(b, n)} = n/b = a$$

Essendo vera la (iii) si ha quindi che $a = 1$ oppure $a = n$.
Quindi n è irriducibile e per 2.10 è primo. ∎

[1] Vedi pagina 47 e lemma 4.17 a pagina 43.

4.2 Congruenze in gruppi, sottogruppi normali

Dato un gruppo G, le relazioni di equivalenza che hanno maggior interesse sono di solito le congruenze, cioè le relazioni compatibili con l'operazione definita su G.
Se R è una congruenza in G allora, secondo la definizione 1.20, si ha che:

$$aRa,\ nR\,1_G \implies (an)R(a) \quad \text{e} \quad (na)R(a)$$

Cioè che le congruenze sono invarianti per moltiplicazione a sinistra e a destra. Grazie a questa proprietà è possibile dare una caratterizzazione importante delle congruenze in un gruppo.

Definizione 4.4 *Sia G un gruppo ed R una congruenza in G.*
La classe $N := [\,1_G\,]_R \subseteq G$ viene detta nucleo della congruenza R.

Ogni congruenza in G è completamente determinata dal suo nucleo che, in realtà, è un sottogruppo di G, come mostra la seguente proposizione.

Proposizione 4.7 *Sia G un gruppo ed R una congruenza in G. Allora:*
(i) *Il nucleo N di R è un sottogruppo di G.*
(ii) $\forall\, a \in G\ \ [\,a\,]_R = Na = aN$ *(ovvero $R = D_N = S_N$)*

***D**imostrazione.* (i.i) Ovviamente $1_G \in [\,1_G\,]_R$
(i.ii) Se $a, b \in [\,1_G\,]_R$ allora $aR1_G,\ bR1_G \implies (ab)R(1_G \cdot 1_G) \implies ab \in [\,1_G\,]_R$.
(i.iii) Se $aR1_G$ allora, siccome $a^{-1}Ra^{-1}$, si ha $(aa^{-1})R(1_G \cdot a^{-1}) \implies a^{-1} \in [\,1_G\,]_R$.
(ii) Proviamo che $\forall\, a \in G,\ \ [\,a\,]_R = Na$. Per ogni b tale che bRa si ha $(ba^{-1})R(1_G)$.
Allora $ba^{-1} \in N \implies b \in Na$. Quindi $[\,a\,]_R \subseteq Na$. Sia ora $na \in Na$.
Allora, poiché $n \in N \Rightarrow nR1_G$, si ha $(na)R(a)$, ovvero $Na \subseteq [\,a\,]_R$.
Procedendo nello stesso modo con aN si arriva a concludere che $aN = Na$. ∎

Quindi se R è una congruenza allora, detto N il suo nucleo, si ha che $R = D_N = S_N$.
Vale anche il viceversa, come mostra la seguente:

Proposizione 4.8 *Sia G un gruppo ed N un sottogruppo tale che $D_N = S_N$.*
Allora, posto $R := D_N = S_N$, R è una congruenza in G avente nucleo N.

***D**imostrazione.* R è di equivalenza per il lemma 4.1. Mostriamo che R è compatibile con il prodotto definito in G. Siano $a, a', b, b' \in G$ tali che aRa' e bRb'.
Allora esistono $n_1, n_2 \in N$ tale che $a' = n_1 a$ e $b' = n_2 b$.
Segue che $a'b' = (n_1 a)(n_2 b) = n_1(an_2)b$ con $an_2 \in aN$.
Siccome $D_N = S_N$ si ha che $aN = Na$ e quindi esiste $n_3 \in N$ tale che $an_2 = n_3 a$.
Allora $a'b' = n_1(n_3 a)b = (n_1 n_3)ab \implies (a'b')R(ab)$.
Infine $[\,1_G\,]_R = N1_G = N$, e quindi N è il nucleo. ∎

Definizione 4.5 *Sia G un gruppo.*
Un sottogruppo $N \leq G$ di G tale per cui $D_N = S_N$ si dice normale (in G).
Si scrive talvolta $N \trianglelefteq G$ per dire che N è un sottogruppo normale di G.

Possiamo quindi tirare le conclusioni ed unificare le due proposizioni nella seguente.

Corollario 4.9 *Sia G un gruppo. L'applicazione $R \mapsto [\,1_G\,]_R$ che associa ad ogni congruenza il suo nucleo N è una bijezione dall'insieme delle congruenze ammesse da G all'insieme dei sottogruppi normali.*

***D**imostrazione.* Per la proposizione 4.7 il nucleo di una congruenza soddisfa $D_N = S_N$ e quindi tale funzione è ben definita. È suriettiva in quanto per la proposizione 4.8 per ogni sottogruppo normale esiste almeno una congruenza. È iniettiva in quanto per 4.7 ogni congruenza è univocamente determinata dal suo nucleo. ∎

Osservazione In ogni gruppo G ci sono dei *sottogruppi normali banali* che sono $\{\,1_G\}$ e G stesso. In un gruppo abeliano tutti i sottogruppi sono ovviamente normali. Inoltre se N è un sottogruppo normale di H ed H è un sottogruppo di G a maggior ragione H è un sottogruppo normale di G.

Definizione 4.6 *Un gruppo privo di sottogruppi normali non banali è detto semplice.*

Definizione 4.7 *Sia G è un gruppo e $g, h \in G$.*
La quantità ghg^{-1} (o $g^{-1}hg$) si chiama coniugato (o trasformato) di h mediante g.

Quando un sottogruppo H di G è normale? Verificare che i laterali destri e sinistri di H coincidano può essere complicato. È allora conveniente un criterio che permetta di stabilire se un sottogruppo è normale partendo dai suoi elementi.

Proposizione 4.10 (Criterio per sottogruppi normali)
Un sottogruppo H di un gruppo G è normale se e solo se per ogni $h \in H$ il coniugato di h mediante un elemento $g \in G$ appartiene ad H. Cioè se è verificata la seguente condizione:

$$\forall\, h \in H,\ \forall\, g \in G \qquad g^{-1}hg \in H$$

***D**imostrazione.* Supponiamo che $\forall\, g \in G,\ Hg = gH$. Allora $\forall\, h_1 \in H$ si ha $h_1 g = g h_2$ per un opportuno $h_2 \in H$. Quindi, moltiplicando a sinistra per g^{-1} si ha:
$g^{-1}h_1 g = h_2 \in H$. Inversamente sia vera la condizione del criterio. Sia un generico $hg \in Hg$. Allora per ipotesi esiste un $h_1 \in H$ tale che:

$$g^{-1}hg = h_1 \implies hg = gh_1 \in gH \implies Hg \subseteq gH$$

D'altra parte dato un generico $gh \in gH$, per ipotesi (applicata a $g^{-1} \in G$), si ha:

$$(g^{-1})^{-1}hg^{-1} = h_1 \implies gh = h_1 g \in Hg \implies gH \subseteq Hg$$

E quindi deve essere $gH = Hg$. ∎

Definizione 4.8 *Sia G un gruppo ed $H, K \subseteq G$ due suoi sottoinsiemi.*
Si definisce prodotto dei sottoinsiemi H e K l'insieme:

$$HK := \{\, hk :\ \forall\, h \in H,\ \forall\, k \in K \,\}$$

Lemma 4.11 *Sia G un gruppo ed $H, K \leq G$ due suoi sottogruppi.*
Allora il prodotto HK è un sottogruppo se e solo se $HK = KH$.
In particolare questo accade se uno dei due sottogruppi è normale.

Osservazione Usando la seguente definizione è possibile notare che se $H \leq G$ e $g \in G$ allora il laterale scritto della forma Hg coincide con il prodotto $H\{g\}$.

Lemma 4.12 *Sia G un gruppo e siano $H, K \leq G$ sottogruppi finiti. Allora:*

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

***D**imostrazione.* Sia $hk \in HK$ e sia $x \in H \cap K$. Allora $hk = (hx)(x^{-1}k)$ con $hx \in H$ e $x^{-1}k \in K$. Quindi ogni hk si può scrivere in almeno $|H \cap K|$ modi. Se $hk = h_1k_1$ allora $h_1^{-1}h = k_1k^{-1} \in H \cap K$. Posto $x := h_1^{-1}h$ si ha che $h = h_1x$ e $k = x^{-1}k_1$. Allora ogni hk si scrive al più in $|H \cap K|$ modi. Segue che $|HK|$ è pari al numero di possibilità per la scelta di $h \in H$ moltiplicato per il numero di possibilità per la scelta di $k \in K$ e diviso per il numero di scritture di ogni elemento. ■

Definizione 4.9 *Sia G un gruppo.*
Si definisce centro di G l'insieme degli elementi di G che commutano con ogni altro elemento di G:

$$Z(G) := \{\, g \in G : \ hg = gh \ \ \forall\, h \in G \,\}$$

Osservazione Si osservi che il centro $Z(G)$ di un gruppo G è sempre un sottogruppo normale. È non vuoto in quanto $1_G \in G$ ed è normale in quanto, per definizione:

$$Z(G) := \{\, g \in G : \ hg = gh \ \ \forall\, h \in G \,\} = \{\, g \in G : \ h = ghg^{-1} \ \ \forall\, h \in G \,\}$$

Cioè è costituito da elementi che soddisfano la condizione del criterio.
In conclusione si ha che per ogni gruppo G, $Z(G) \trianglelefteq G$.

Ovviamente dalla definizione di gruppo abeliano si ha che:

Lemma 4.13 *Sia G un gruppo. Allora $Z(G) = G$ se e solo se G è abeliano.*
Se $Z(G) = \{\, 1_G\}$ si dice che G è altamente non abeliano.

Esempio Se si pone $G = S_3 = \mathfrak{S}_3$ (gruppo delle permutazioni di un insieme con tre elementi) e si considera l'operazione di composizione di permutazioni si ottiene subito che $Z(S_3) = \{\, \mathrm{id}\}$. Quindi S_3 è altamente non abeliano.

4.3 Omomorfismi e gruppi quoziente

Definizione 4.10 *Siano G_1 e G_2 due gruppi.*
Una applicazione $F : G_1 \to G_2$ si dice morfismo di gruppi, o omomorfismo se conserva il prodotto. Cioè se vale la seguente condizione:

$$\forall\, a,\, b \in G_1 \qquad F(ab) = F(a)F(b)$$

Se F è iniettiva si dice che è un monomorfismo, se è suriettiva si dice che è un epimorfismo, se è bijettiva si dice che è un isomorfismo. Se $G_1 = G_2$ ed F è una bijezione si dice che F è un automorfismo. L'insieme degli automorfismi di un gruppo G si indica con $\mathrm{Aut}(G)$.

Lemma 4.14 *Sia F un morfismo tra i gruppi G ed H. Allora:*
(i) $F(1_G) = 1_H$
(ii) $\forall\, q \in G \quad F(q^{-1}) = (F(q))^{-1}$

***D**imostrazione.* (i) Si ha che $F(1_G) = F(1_G \cdot 1_G) = F(1_G) \cdot F(1_G)$. Si può quindi scrivere $1_H \cdot F(1_G) = F(1_G) \cdot F(1_G)$. Moltiplicando a destra per $(F(1_G))^{-1} \in H$ si ottiene l'asserto per la legge di cancellazione (3.3).
(ii) Per il primo punto $F(1_G) = F(g \cdot g^{-1}) = F(g) \cdot F(g^{-1})$ e quindi $F(g^{-1})$ è l'inverso destro di $F(g)$ in H. Per l'unicità dell'inverso in un gruppo (1.9) si ha che $F(g^{-1}) = (F(g))^{-1}$. ∎

Definizione 4.11 *Se esiste un isomorfismo tra due gruppi G_1 e G_2 si dice che sono isomorfi e si scrive $G_1 \backsimeq G_2$.*

Lemma 4.15 *La composizione di omomorfismi è un omomorfismo. In particolare la composizione di monomorfismi è un monomorfismo, la composizione di epimorfismi è un epimorfismo e la composizione di isomorfismi è un isomorfismo.*

***D**imostrazione.* Se $S : G_1 \to G_2$ e $T : G_2 \to G_3$ sono omomorfismi si ha:

$$(T \circ S)(ab) = T(S(ab)) = T(S(a)S(b)) = T(S(a))T(S(b)) = (T \circ S)(a) \cdot (T \circ S)(b)$$

Il resto della proposizione segue dalle proprietà della funzione composta. ∎

Lemma 4.16 *La relazione di isomorfismo $\backsimeq$ che associa due gruppi se sono isomorfi è una relazione di equivalenza nell'insieme di tutti i gruppi.*

***D**imostrazione.* (i) La riflessività segue dal fatto che per ogni gruppo G l'applicazione identica è un isomorfismo da G in G e quindi $G \backsimeq G$.
(ii) La simmetria segue immediatamente dal fatto che la bijettività è condizione necessaria e sufficiente per l'invertibilità di una funzione; è inoltre tale inversa è un morfismo perché: $F^{-1}(xy) = F^{-1}(F(a)F(b)) = F^{-1}(F(ab)) = ab = F^{-1}(x)F^{-1}(y)$.
(iii) La transitività segue dal lemma precedente. ∎

Lemma 4.17 *Siano G, H gruppi ed $f : G \to H$ un omomorfismo. Allora:*
(i) *Se K è un sottogruppo di G, $f(K)$ è un sottogruppo di H.*
(ii) *Se T è un sottogruppo di H, $f^{-1}(T)$ è un sottogruppo di G.*

***D**imostrazione.* (i) Per il lemma 4.14, $1_H \in f(K)$ e quindi $f(K) \neq \emptyset$.
Se $h_1, h_2 \in f(K)$ allora esistono $k_1, k_2 \in K$ tali che $h_1 = f(k_1)$ e $h_2 = f(k_2)$.
Allora applicando il lemma 4.14 e il criterio 3.5 si ha quanto richiesto:
$h_1 h_2^{-1} = f(k_1)(f(k_2))^{-1} = f(k_1)f(k_2^{-1}) = f(k_1 k_2^{-1}) \in f(K)$.
(ii) In modo analogo per 4.14, $1_G \in f^{-1}(T)$ e quindi $f^{-1}(T) \neq \emptyset$.
Se $g_1, g_2 \in f^{-1}(T)$ allora esistono h_1, h_2 tale che $h_1 = f(g_1)$ ed $h_2 = f(g_2)$.
Ma allora $f(g_1 g_2^{-1}) = f(g_1)(f(g_2))^{-1} = h_1 h_2^{-1} \in T$ in quanto T è un gruppo.
Segue che $gg^{-1} \in f^{-1}(T)$, e quindi la tesi per 3.5. ∎

Lemma 4.18 *Siano G, H gruppi ed $f : G \to H$ un omomorfismo. Allora:*
(i) *La preimmagine $f^{-1}(K)$ di un sottogruppo normale K di H è un sottogruppo normale di G.*
(ii) *Se f è un epimorfismo, l'immagine $f(N)$ di un sottogruppo normale N di G è un sottogruppo normale di H.*

***D**imostrazione.* (i) Usiamo il criterio per i sottogruppi normali 4.10. Sia $u \in F^{-1}(K)$.
Allora $\exists\, k \in K : k = f(u)$. Per ogni $g \in G$ esiste $h \in H$ tale che $h = f(g)$. Quindi si ha che $f(g^{-1}ug) = (f(g))^{-1}f(u)f(g) = h^{-1}kh$. Essendo K normale e 4.10 condizione necessaria per la normalità si ha che $h^{-1}kh \in K$. Allora $g^{-1}ug \in f^{-1}(K)$.
Essendo 4.10 sufficiente per la normalità si ha l'asserto.
(ii) Sia $h \in H$ e $s \in f(N)$. Allora si ha $s = f(n)$ per un opportuno $n \in N$.
Per la suriettività di f si ha anche $h = f(g)$ per un opportuno $g \in G$.
Allora $h^{-1}sh = f(g^{-1})f(n)f(g) = f(g^{-1}ng)$. Ancora una volta essendo N normale si ha $g^{-1}ng \in N$. Quindi $h^{-1}sh \in F(N)$, e dunque $F(N)$ è normale. ∎

Se G è un gruppo ed R è una congruenza, per la proposizione 4.7 l'insieme quoziente G/R (insieme delle classi di equivalenza) coincide con l'insieme dei laterali destri o sinistri del nucleo $N = [\,1_G\,]_R$. La stessa proposizione 4.7 può essere letta dicendo che il nucleo di una congruenza R in G (classe dell'unità) è un sottogruppo normale di G e la classe di equivalenza $[\,a\,]_R$ coincide con il laterale destro (o sinistro) Na. Data questa caratterizzazione si preferisce allora introdurre la seguente terminologia.

Definizione 4.12 *Sia R una congruenza in un gruppo G, con nucleo $N := [\,1_G\,]_R$. L'insieme quoziente G/R sarà denotato con G/N e si parlerà di gruppo quoziente*[1] *rispetto al suo sottogruppo normale N.*

Per la proposizione 4.8, se N è un sottogruppo normale di G allora la relazione di equivalenza che associa due elementi se stanno nello stesso laterale destro (o sinistro) è una congruenza il cui nucleo è N. Segue che l'insieme quoziente G/N secondo la definizione data è esattamente l'insieme quoziente $G/D_N = G/S_N$. In generale si può quindi parlare di *gruppo quoziente rispetto ad un sottogruppo normale.*

Si ricorda che, sulla base di quanto descritto nella proposizione 1.10 a pagina 14, se $N \trianglelefteq G$ allora resta definita in G un'operazione indotta dal prodotto di G che opera associando alle classi di equivalenza di due rappresentanti $a, b \in G$ la classe del prodotto ab. Il fatto che sia ben definita tale operazione come già visto segue proprio

[1] Gruppo per il teorema seguente.

dal fatto che la relazione D_N è una congruenza. L'operazione indotta si leggerà quindi usando la nuova terminologia nel seguente modo:

$$Na \cdot Nb = Nab \qquad \text{cioè} \qquad [\,a\,]_{D_N} \cdot_{D_N} [\,b\,]_{D_N} = [\,a \cdot b\,]_{D_N}$$

Che altro non è che una riscrittura di quanto detto a pagina 14.
Si parlerà quindi di *prodotto di laterali* nel senso appena precisato.

Teorema 4.19 (gruppo quoziente ed epimorfismo canonico)
Sia G un gruppo ed N un sottogruppo normale di G. Allora:
(i) *L'insieme quoziente G/N è un gruppo rispetto all'operazione indotta dal prodotto definito in G.*
(ii) *La proiezione canonica $\pi : G \to G/N$ è un epimorfismo*

$$\forall\, a \in G \qquad a \overset{\pi}{\longmapsto} Na \ \in G/N$$

detto epimorfismo canonico.

***D**imostrazione.* (i) Il prodotto di laterali è associativo (proprietà equazionale).
$N1_G = N$ funziona da unità in G/N. Il laterale Na^{-1} funziona da inverso di Na.
(ii) Ovviamente π è suriettiva ($\forall\, Na \in G/N,\ a \in Na$).
Inoltre $\pi(ab) = Nab = Na \cdot Nb = \pi(a) \cdot \pi(b)$ ■

Osservazioni

1. Si ponga attenzione sul fatto che per dimostrare che *l'insieme quoziente G/N* è un *gruppo* ha giocato un ruolo essenziale il fatto che N sia un sottogruppo normale. Infatti è la normalità di N a garantire che la relazione D_N (o S_N) sia una congruenza ed è il fatto che D_N sia una congruenza a garantire il fatto che l'operazione indotta su G/N sia ben definita. Senza l'ipotesi di normalità non è detto che si possa indurre una operazione sull'insieme quoziente dandogli la struttura di gruppo.
2. Se $Na \in G/N$ allora la preimmagine mediante π di Na è ovviamente costituita dagli elementi che fanno parte del laterale Na, cioè gli elementi della forma na per un qualche $n \in N$.
3. Se G è un gruppo e $\{\,1_G\}$ è il suo sottogruppo normale banale il gruppo quoziente $G/\{\,1_G\}$ è isomorfo a G stesso in quanto costituito dalle classi laterali dell'unità:

   $$G/\{\,1_G\} = \{\{\,1_G\}g :\ g \in G\} = \{\{\,g\} :\ g \in G\}$$

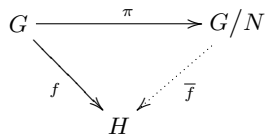
   E quindi l'epimorfismo canonico $\pi : G \to G/\{\,1_G\}$ è una bijezione.

Dati due gruppi G, H e un sottogruppo normale $N \trianglelefteq G$ ed un (omo)morfismo $f : G \to H$ per il teorema d'omomorfismo per classi di insiemi (teorema 1.6 pag.10) esiste ed è univocamente determinata un'applicazione $\overline{f} : G/N \to N$, definita da $\overline{f}(Na) = f(a)$, tale per cui $f = \overline{f} \circ \pi$.

Teorema 4.20 (Teorema d'omomorfismo per i gruppi)
Siano G ed H gruppi e $f : G \to H$ un omomorfismo. Allora:
(i) *La relazione di equivalenza R associata ad f è una congruenza in G.*
(ii) *Se N è il nucleo di R e π è l'epimorfismo canonico da G in G/N esiste uno ed un solo omomorfismo $\overline{f} : G/N \to H$ tale che:*

$$f = \overline{f} \circ \pi \qquad \textit{(Proprietà universale dell'epimorfismo canonico)}$$

Cioè tale da rendere commutativo il seguente diagramma:



$\overline{f}$ è sempre un monomorfismo ed è un isomorfismo se e solo se f è un epimorfismo.

***D**imostrazione.* (i) Sia $R := R_f$. Supponiamo che aRa', bRb' con $a, a', b, b' \in G$. Allora $aRa' \Rightarrow f(a) = f(a')$, $bRb' \Rightarrow f(b) = f(b')$. Quindi, essendo f un morfismo, si ha $f(ab) = f(a)f(b) = f(a')f(b') = f(a'b')$, cioè $(ab)R(a'b')$.
(ii) Per il teorema d'omomorfismo per classi di insiemi esiste $\overline{f} : G/N \to H$ definita da $\overline{f}(Na) = f(a)$ tale che $f = \overline{f} \circ \pi$. Resta da provare che $\overline{f}$ è un morfismo. Ma infatti:

$$\overline{f}(Na \cdot Nb) = \overline{f}(Nab) = f(ab) = f(a)f(b) = \overline{f}(Na)\overline{f}(Nb)$$

Il resto del teorema segue da 1.6. ∎

Definizione 4.13 *Siano G ed H gruppi. Sia $f : G \to H$ un morfismo.*
Il nucleo N della congruenza associata al morfismo f si dice nucleo di f e si pone:

$$\ker f := N = \{g \in G : \ f(g) = f(1_H) = 1_H\}$$

Osservazioni
I teoremi precedenti provano che:

1. Se f è un morfismo $\ker f$ è un sottogruppo normale di G. Infatti è il nucleo della relazione di equialenza associata ad f che per 4.20 è una congruenza. Quindi per la proposizione 4.7 è un sottogruppo normale di G.
2. Ad ogni sottogruppo normale N di un gruppo G corrisponde un epimorfismo (e.g. π) $G \to G/N$ avente come nucleo N (conseguenza immediata di 4.19).
3. Se H è un gruppo immagine epimorfa di G allora $H \backsimeq G/\ker f$. Infatti, se $f : G \to H$ è l'epimorfismo in questione, per il teorema d'omomorfismo 4.20 la funzione $\overline{f} : G/\ker f \to H$ è un isomorfismo.

Lemma 4.21 *Siano G, H gruppi ed $f : G \to H$ un morfismo.*
Allora f è un monomorfismo se e solo se $\ker f = \{1_G\}$.

***D**imostrazione.* Se f è iniettiva allora $f(g) = 1_H = f(1_G) \implies g = 1_G$.
Viceversa se $\ker f = \{1_G\}$ allora $f(g_1) = f(g_2) \implies f(g_1)(f(g_2))^{-1} = f(g_2)(f(g_2))^{-1}$ e quindi $f(g_1 g_2^{-1}) = 1_H$, cioè $g_1 g_2^{-1} \in \ker f$. Allora essendo $\ker f = \{1_G\}$ deve essere $g_1 g_2^{-1} = 1_G$, da cui $g_1 = g_2$. ∎

Teorema 4.22 (Teorema di corrispondenza)
Sia G un gruppo ed $N \trianglelefteq G$. Allora ogni sottogruppo del gruppo quoziente G/N è della forma H/N per qualche $H \leq G$ tale che $N \subseteq H$. Inversamente se H è un sottogruppo di G contenente N allora $H/N \leq G/N$. Infine la corrispondenza tra sottogruppi di G/N e sottogruppi di G contenenti N è una bijezione. Tale bijezione mappa sottogruppi normali di G/N in sottogruppi normali di G contenenti N.

***D**imostrazione.* Sia $\overline{H}$ un sottogruppo del gruppo quoziente G/N. Allora $\overline{H}$ è l'insieme dei laterali destri (o sinistri) di N in G. Ad esempio $\overline{H} = \{\, gN : \ g \in G \,\}$. Definiamo il sottoinsieme $\beta(\overline{H})$ di G ponendo:

$$\beta(\overline{H}) := \{\, g \in G : \ gN \in \overline{H} \,\}$$

Ovviamente si ha che $N \subseteq \beta(\overline{H})$ in quanto $1_{G/N} = N \in \overline{H}$ e quindi $N \subseteq \beta(1_{G/N})$. Inoltre $\beta(\overline{H})$ è un sottogruppo di G in quanto:
(i) $1_G \in \beta(\overline{H})$ perché $1_G N = N \in \overline{H}$.
(ii) $x, y \in \beta(\overline{H}) \implies xN, yN \in \overline{H} \implies xN \cdot yN = xyN \in \overline{H} \implies xy \in \beta(\overline{H})$.
(iii) Se $x \in \beta(\overline{H})$ allora $(xN)^{-1} = x^{-1}N \in \overline{H}$, cioè $x^{-1} \in \beta(\overline{H})$. Inversamente sia H un sottogruppo di G contenente N. Definiamo l'insieme:

$$\alpha(H) := \{\, hN : \ h \in H \,\} \ \subseteq G/N$$

Si ha che $\alpha(H) \leq G/N$ in quanto:
(i) $1_G \in H \implies 1_G N = N = 1_{G/N} \in \alpha(H)$.
(ii) Se $\overline{x}, \overline{y} \in \alpha(H)$ allora $\overline{x} = xN$ e $\overline{y} = yN$. Segue che $\overline{xy} = xN \cdot yN = xyN \in \alpha(H)$.
(iii) Se $\overline{x} \in \alpha(H)$ allora $\overline{x} = xN$. Quindi $\overline{x}^{-1} = (xN)^{-1} = x^{-1}N \in \alpha(H)$.
Mostriamo che l'applicazione $\alpha : X \to Y$ dall'insieme X dei sottogruppi di G contenenti N e l'insieme dei sottogruppi di G/N è una bijezione. Basta in realtà far vedere che β è l'inversa di α. Ma infatti, se $N \subseteq H \leq G$ $(H \in X)$ si ha che $(\beta \circ \alpha)(H) = \beta(\alpha(H)) = \beta(H/N) = H$. D'altra parte se $\overline{H} \leq G/N$ allora si ha $(\alpha \circ \beta)(\overline{H}) = \alpha(\beta(\overline{H})) = \alpha(\{\, g \in G : \ gN \in \overline{H} \,\}) = \{\, gN : gN \in \overline{H} \,\} = \overline{H}$.
Infine se $N \leq H \trianglelefteq G$ si ha che $\alpha(H) \trianglelefteq G/N$. Infatti $\forall\, gN \in G/N$; $\forall\, hN \in \alpha(H)$ si ha $(gN)(hN)(gN)^{-1} = (ghg^{-1})N$ e $ghg^{-1} \in H$. Se $\overline{H} \trianglelefteq G/N$ si ha che $\beta(\overline{H}) \trianglelefteq G$ in quanto $\forall\, k \in G \ \ (kgk^{-1})N = (kN)(gN)(kN)^{-1} \in \beta(\overline{H})$. ∎

4.4 Classificazione dei gruppi ciclici

Vediamo un esempio di applicazione del teorema di omomorfismo. Poniamo $G = (\mathbb{Z}, +)$ gruppo additivo degli interi relativi e $H = \langle a \rangle$ sottogruppo ciclico generato da a di un generico gruppo moltiplicativo. La funzione potenza $f : \mathbb{Z} \to \langle a \rangle$ che associa ad ogni intero relativo r la potenza r-esima di a, a^r è un'applicazione suriettiva in quanto per 3.9 ogni elemento di $\langle a \rangle$ è potenza di a. Inoltre è un morfismo (e quindi un epimorfismo) in quanto, per le proprietà della potenza (vedi 3.4 pagina 28):

$$f(r+s) = a^{r+s} = a^r a^s = f(r)f(s)$$

Il nucleo di f è quindi $\ker f = \{\, r \in \mathbb{Z} :\ f(r) = a^r = 1_H \,\}$.
Ci sono quindi due possibilità per l'ordine di a: $o(a) = \infty$ oppure $o(a) = n < \infty$.

1. Nel caso in cui $o(a) = \infty$ per la proposizione 3.10 pagina 31 la funzione f è iniettiva. Quindi per il lemma 4.21 si ha[1] $\ker f = \{\, 0\}$. Per il teorema di omomorfismo si ha quindi che $\mathbb{Z}/\ker f = \mathbb{Z}/\{\, 0\} \backsimeq \langle a \rangle$.
   Essendo che $\mathbb{Z}/\{\, 0\} \backsimeq \mathbb{Z}$ segue che $\langle a \rangle \backsimeq \mathbb{Z}$. Si è quindi provato che *ogni sottogruppo ciclico infinito è isomorfo al gruppo additivo degli interi relativi.*
2. Nel caso in cui $o(a) = n < \infty$ si ha $\ker f = \{\, r \in \mathbb{Z} :\ a^r = 1_H = a^0 \}$. Per la proposizione 3.10 pagina 31 $a^r = a^0$ se e solo se $r \equiv 0_{(n)}$, cioè se e solo se $r = hn$ per qualche $h \in \mathbb{Z}$. Quindi $\ker f = \{\, nh :\ h \in \mathbb{Z}\} = n\mathbb{Z}$. Allora il teorema di omomorfismo dice che $\mathbb{Z}/n\mathbb{Z} \backsimeq \langle a \rangle$. Si noti che $\mathbb{Z}/n\mathbb{Z}$ è esattamente l'insieme delle classi resto modulo n in quanto: $n\mathbb{Z} + a = \{\, nh + a :\ h \in \mathbb{Z}\,\} = [\, a\,]_n$ e quindi $\mathbb{Z}/n\mathbb{Z} = \{\, n\mathbb{Z} + a :\ a \in \mathbb{Z}\,\} = \{\, n\mathbb{Z},\ n\mathbb{Z}+1,\ \ldots,\ n\mathbb{Z}+(n-1)\,\}$. Segue che l'operazione indotta nel gruppo quoziente data da:

   $$(n\mathbb{Z} + a) + (n\mathbb{Z} + b) = n\mathbb{Z} + (a + b)$$

   coincide con la comune operazione $[\, a\,]_n + [\, b\,]_n = [\, a + b\,]_n$.
   Si è quindi provato che *ogni gruppo ciclico di ordine n è isomorfo al gruppo additivo delle classi resto modulo n.*

Si può quindi riassumere quanto ottenuto nella seguente proposizione:

Corollario 4.23 *A meno di isomorfismi i gruppi ciclici sono due: il gruppo additivo degli interi relativi e il gruppo additivo delle classi resto modulo n.*

Corollario 4.24 *Un gruppo finito G con un numero primo di elementi è ciclico. Inoltre $G \backsimeq \mathbb{Z}/p\mathbb{Z}$ e ogni elemento di G che non sia l'unità ha periodo p.*

***D**imostrazione.* Avendo G un numero primo di elementi ($|G| = p$) in particolare $|G| \geq 2$. Sia allora $1_G \neq a \in G$ un elemento diverso dall'unità. Consideriamo allora il sottogruppo $\langle a \rangle \leq G$. a ha periodo maggiore di 1 per costruzione. Per il teorema di Lagrange (4.4) $o(a) \mid p$. Segue che deve essere $o(a) = p$. Allora G é il gruppo ciclico (di ordine p) generato da a e per il corollario 4.23 è isomorfo a $\mathbb{Z}/p\mathbb{Z}$. ∎

[1] Attenzione alla notazione additiva.

4.5 Teoremi di isomorfismo per i gruppi

Vediamo ora i due teoremi di isomorfismo per i gruppi.

Teorema 4.25 (Primo teorema d'isomorfismo)
Sia G un gruppo ed N, H due sottogruppi di G. Sia N normale in G. Allora N è un sottogruppo normale del gruppo NH, $N \cap H$ è un sottogruppo normale di H e si ha:

$$(NH)/N \backsimeq H/(H \cap N)$$

***D**imostrazione.* Essendo N normale in G a maggior ragione è normale in $NH \subseteq G$. $N \cap H$ è un sottogruppo di G per il lemma 3.7 pagina 30 ed è ovviamente normale in G. Per dimostrare l'isomorfismo applichiamo il teorema di omomorfismo. Sia l'applicazione $f : H \to NH/N$ definita ponendo:

$$\forall\, h \in H \qquad h \overset{f}{\longmapsto} Nh$$

Tale applicazione è suriettiva in quanto $\forall\, nh \in NH \;\; Nnh = Nh$ e quindi ogni elemento di NH/N può essere scritto della forma Nh. Inoltre f conserva il prodotto in quanto: $f(h_1h_2) = Nh_1h_2 = Nh_1 \cdot Nh_2 = f(h_1)f(h_2)$. Dunque f è un epimorfismo da H in NH/N. Per il teorema d'omomorfismo allora si ha:

$$H/\ker f \backsimeq NH/N$$

D'altra parte $\ker f = \{\, h \in H :\; f(h) = Nh = 1_{NH/N} = N \,\} = H \cap N$. ∎

Teorema 4.26 (Secondo teorema d'isomorfismo)
Sia G un gruppo ed $N \trianglelefteq H \trianglelefteq G$ due sottogruppi normali di G. Allora H/N è un sottogruppo normale del gruppo quoziente G/N e si ha:

$$(G/N)/(H/N) \backsimeq G/H$$

***D**imostrazione.* Consideriamo l'applicazione $f : G/N \to G/H$ definita da:

$$Ng \overset{f}{\longmapsto} Hg$$

f è ben definita in quanto se x è un altro rappresentante ($Nx = Ng$) allora $x = ng$ per qualche $n \in N$. Allora si ha $f(Nx) = Hx = Hng = Hg$ poiché $n \in N \subseteq H$. f è suriettiva per costruzione e conserva il prodotto: $f(Ng_1Ng_2) = f(Ng_1g_2) = Hg_1g_2 = Hg_1Hg_2 = f(Ng_1)f(Ng_2)$. Dunque per il teorema d'omomorfismo:

$$(G/N)/\ker f \backsimeq G/H$$

D'altra parte $\ker f = \{\, Ng \in G/N :\; f(Ng) = Hg = 1_{G/H} = H \,\}$.
Essendo che $Hg = H \iff g \in H$ si ha $\ker f = \{\, Nh :\; h \in H \,\} = H/N$. ∎

Osservazione I due teoremi di isomorfismo dicono sostanzialmente che valgono due "leggi di cancellazione". La prima afferma che quando $N \trianglelefteq G$ e $H \leq G$ allora quando si considera il gruppo quoziente $(NH)/N$ si può cancellare N ma rimane a denominatore l'intersezione $H \cap N$. La seconda legge dice che se $N \trianglelefteq G$ e $H \trianglelefteq G$ con $N \subseteq H$ allora dal gruppo quoziente $(G/N)/(H/N)$ si può cancellare N.

4.6 Azioni di gruppo

Definizione 4.14 *Sia G un gruppo e X un insieme non vuoto.*
Si dice azione di G su X un'applicazione $G \times X \to X$, $(g, x) \mapsto g \cdot x$ tale che:
(i) $\forall\, x \in X; \quad 1_G \cdot x = x$.
(ii) $\forall\, g, h \in G;\ \forall\, x \in X; \quad (gh) \cdot x = g \cdot (h \cdot x)$.
Se è assegnata un'azione di G su X si dice anche che X è un G-insieme (sinistro).

Osservazione Un azione $G \times X \to X$ si dice *banale* se $\forall\, g \in G;\ \forall\, x \in X; \ \ g \cdot x = x$ cioè se l'azione di ogni elemento di G *fissa* ogni elemento di X.

Lemma 4.27 (Rappresentazione di permutazione)
Data un'azione $G \times X \to X$ e $g \in G$ resta definita l'applicazione $\sigma_g : X \to X$ come:

$$\sigma_g :\ x \longmapsto g \cdot x \qquad (\sigma_g \in S_X)$$

Tale applicazione è una bijezione di X in sé. L'applicazione $\sigma : G \to S_X$ definita da:

$$\forall\, g \in G \ \ g \overset{\sigma}{\longmapsto} \sigma_g \in S_X$$

È un morfismo dal gruppo G nel gruppo simmetrico S_X. Vi è inoltre una bijezione fra l'insieme delle azioni di un gruppo G sull'insieme X e l'insieme degli omomorfismi del gruppo G nel gruppo simmetrico S_X.

***D**imostrazione.* L'applicazione σ_g è iniettiva in quanto $gx_1 = gx_2 \implies g^{-1}(gx_1) = g^{-1}(gx_2) \implies x_1 = x_2$, dove si sono usate in ordine le proprietà (ii) e (i) dell'azione. σ_g è suriettiva in quanto $\forall\, y \in X :\ y = g(g^{-1}y) = g \cdot x$ per un elemento $x \in X$.
L'applicazione $\sigma : G \to S_X$ definita sopra è un morfismo di gruppi. Infatti $\sigma_{g_1 g_2}(x) = (g_1 g_2)x = g_1(g_2 x) = \sigma_{g_1}(\sigma_{g_2}(x))$ e quindi $\sigma(g_1 g_2) = \sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2} = \sigma(g_1) \circ \sigma(g_2)$. Allora l'applicazione Φ che associa ad ogni azione $G \times X \to X$ il morfismo σ definito come sopra è una applicazione tra l'insieme delle azioni di un gruppo G sull'insieme degli omomorfismi $G \to S_X$ Viceversa sia $f : G \to S_X$ un omomorfismo di gruppi. Allora è definita un'azione $G \times X \to X$ definita da $g \cdot x = f(g)(x)$. Infatti si ha che (i) $1_G x = f(1_G)(x) = \mathrm{id}_X(x) = x$ e (ii) $(gh)x = f(gh)(x) = (f(g) \circ f(h))(x) = f(g)(f(h)(x)) = g(hx)$. L'applicazione che associa ad ogni morfismo $G \to S_X$ l'azione f definita come sopra è l'inversa di Φ, e quindi si ha l'asserto. ∎

Dato un insieme X e un gruppo G, un morfismo di gruppi $\sigma : G \to S_X$ si dice anche *rappresentazione di permutazione* di G su X.

Definizione 4.15 *Un'azione $G \times X \to X$ di G su X si dice:*
(i) *Transitiva se $\forall\, x, y \in X$ esiste $g \in G$ tale che $g \cdot x = y$.*
(ii) *Fedele se per ogni $g \neq 1_G$ l'applicazione $\sigma_g : X \to X$ definita da $\sigma_g := g \cdot x$ non è l'applicazione identica. Analogamente dato il morfismo $\sigma : G \to S_X$ l'azione è fedele se $\ker \sigma = \{\, 1_G \}$ cioè se σ è iniettivo (monomorfismo).*
Si dice anche in questi casi che σ è fedele.

Definizione 4.16 *Sia un'azione $G \times X \to X$ di un gruppo G su X.*
Fissato un $x \in X$ poniamo:
(i) $Gx := \{\, g \cdot x :\ \forall\, g \in G \,\} \subseteq X$.
(ii) $G_x := \{\, g \in G :\ g \cdot x = x \,\} \leq G$ *(elementi di G che fissano x).*
Diremo che Gx è la G-orbita su X contenente x.
Diremo che G_x è lo stabilizzatore del punto x in G.

Osservazioni

1. Lo stabilizzatore G_x di $x \in X$ è un sottogruppo normale di G. Infatti $1_G \cdot x = x$ e se $a, b \in G_x$ allora si ha $(ab^{-1}) \cdot x = (ab^{-1})(b \cdot x) = a \cdot ((b^{-1}b) \cdot x) = a \cdot x = x$. Quindi $ab^{-1} \in G_x$ e la tesi segue dal criterio 3.5. È normale in G in quanto è il nucleo del morfismo σ (la relazione di equivalenza associata ad un morfismo è una congruenza il cui nucleo è quindi normale in G per la proposizione 4.7).
2. L'omomorfismo σ definito nel lemma 4.27 non è in generale iniettivo o suriettivo. Se però $\ker \sigma = \{ 1_G \}$, ovvero σ è fedele (l'azione definita da $(g, x) \mapsto \sigma(g)(x)$ è fedele), allora si ha che $G \backsimeq \sigma(G)$.

Lemma 4.28 *La relazione $\sim$ su G definita ponendo $\forall\, x, y \in X;\ x \sim y$ sse $\exists\, g \in G$ tale che $y = g \cdot x$ è una relazione di equivalenza su X. In particolare una azione è transitiva se e solo se vi è una sola orbita di G su X.*

***D**imostrazione.* Si ha $x = 1_G \cdot x$. Se $y \sim x$ allora $y = g \cdot x$. Segue che $g^{-1} \cdot y = (g^{-1}g) \cdot x = x$. Infine se $y = g_1 \cdot x$ e $z = g_2 \cdot y$ allora $z = g_2 \cdot (g_1 \cdot x) = (g_1 g_2) \cdot x$. Quindi la relazione $\sim$ partisce l'insieme X in classi di equivalenza disgiunte $[\, x \,]_\sim = Gx$ che coincidono con le orbite degli elementi $x \in X$. ■

Proposizione 4.29 (Lunghezza orbita = indice stabilizzante)
Sia un'azione $G \times X \to X$ del gruppo G (finito o no) sull'insieme X (finito o no). Sia fissato un $x \in X$. Allora la cardinalità dell'orbita $|Gx|$ è pari all'indice dello stabilizzante di x in G:

$$|Gx| = (G : G_x)$$

In particolare se G è finito si ha che $|Gx| = |G|/|G_x|$ e quindi $|Gx|$ divide $|G|$.

***D**imostrazione.* Se $g, h \in G$ allora $g \cdot x = h \cdot x$ se e solo se $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (h \cdot x)$ che avviene se e solo se $x = (g^{-1}h) \cdot x$ che vuol dire che l'elemento $g^{-1}h \in G$ fissa x, cioè $g^{-1}h \in G_x$. Moltiplicando a destra per g^{-1} si ottiene $hG_x = gG_x$. Quindi ci sono tante immagini distinte quanti sono i laterali dello stabilizzatore. ■

Il seguente corollario si chiama normalmente *equazione delle orbite*.

Corollario 4.30 (Equazione delle orbite) *Sia $|X| = n < \infty$. Sia $\{ X_1, \dots X_r \}$ la partizione di X in G-orbite. Sia $\{ x_1, \dots, x_r \}$ un sistema completo di rappresentanti per le G-orbite X_i. Allora:*

$$|X| = \sum_{i=1}^{r} |Gx| = \sum_{i=1}^{r} (G : G_{x_i})$$

***D**imostrazione.* Essendo X unione disgiunta degli $X_1, \dots X_r$ si ha:

$$X = \bigcup_{i=1}^{\bullet\, r} X_i \implies |X| = \sum_{i=1}^{r} |X_i| = \sum_{i=1}^{r} (G : G_{x_i})$$

In quanto per il teorema precedente la lunghezza di ogni orbita X_i è pari all'indice dello stabilizzante G_{x_i}. ■

4.6.1 Esempio: rappresentazione regolare sinistra

Un esempio importante del caso generale preso in cosiderazione è il caso in cui $X = G$. In questo caso il lemma appena visto dice che esiste una bijezione tra l'insieme delle azioni di G su G e il gruppo simmetrico S_G. Si consideri l'azione $G \times G \to G$ definita da:

$$\forall\, g, h \in G \quad (g, h) \longmapsto gh \qquad \text{(Prodotto a sinistra } g \cdot h \text{ in } G)$$

È un'azione in quanto[1] (i) $1_G \cdot h = 1_G h = h$ e (ii) $(g_1 g_2) \cdot h = g_1 g_2 h = g_1(g_2 h) = g_1 \cdot (g_2 \cdot h)$. Per il lemma 4.27 questa azione realizza un omomorfismo $\sigma : G \to S_G$ che associa ad ogni $g \in G$ l'applicazione $\sigma_g : G \to G$ definita da $\sigma_g(h) := gh$ (la moltiplicazione a sinistra per g). Il nucleo di σ è dato da tutti e soli gli elementi g tali per cui $\sigma_g = 1_{S_G} = \mathrm{id}_G$, cioè da quegli elementi tali per cui $\forall\, h \in G,\ gh = h$. In particolare per $h = 1_G$ si ottiene $g = 1_G$. Quindi $\ker \sigma = \{\, 1_G \}$, ovvero σ è fedele. Detto in altri termini si ha che G è isomorfo a $\sigma(G)$ che, per il lemma 4.17, è un sottogruppo del gruppo totale S_G. Si ha cioè:

$$G \backsimeq \sigma(G) \leq S_G$$

L'argomento mostra in realtà che se $g \neq 1_G$ la permutazione σ_g non fissa alcun elemento di G (è priva di punti fissi). Infatti σ_g corrisponde alla moltiplicazione a sinistra. Dati due elementi $a, b \in G$ esiste $g \in G$ tale che $\sigma_g(a) = b$. Infatti basta prendere $g := ba^{-1}$ perché $\sigma_{ba^{-1}}(a) = (ba^{-1})a = b$. Questa caratteristica si dice anche che G *opera transitivamente* su se stesso mediante σ. Si parla quindi in questo caso di *rappresentazione regolare sinistra* di G. Considerando l'esempio precedente nel caso particolare in cui $X = G$ e $|G| = n < \infty$ si ha il classico *Teorema di Cayley*:

Teorema 4.31 (di Cayley)
Sia G un gruppo finito di ordine n. Allora esiste un monomorfismo $\sigma : G \to S_n$ tale che il gruppo di permutazioni $\sigma(G) \leq S_n$ (che è isomorfo a G) è transitivo in G e ogni permutazione $\sigma(g) = \sigma_g$ con $g \neq 1_G$ non ha punti fissi su G.

Essendo l'azione di moltiplicazione a sinistra transitiva, esiste un'unica orbita $Gh = \{\, gh = \sigma_g(h) :\ \forall\, g \in G \,\}$. Lo stabilizzatore è banale: $G_h = \{\, 1_G \}$. Se consideriamo la restrizione della rappresentazione regolare di G al sottogruppo ciclico generato da $g \in G$ allora si ha, per la proposizione 4.29:

$$\forall\, x \in G \quad |\langle g \rangle\, x| = \frac{|\langle g \rangle|}{\left|\langle g \rangle_x\right|} = |\langle g \rangle| = o(g)$$

In quanto $\left|\langle g \rangle_x\right| = 1$. Quindi in questo caso quindi ogni orbita $\langle g \rangle\, x$ ha lunghezza pari al periodo dell'elemento $o(g)$.

4.6.2 Esempio: rappresentazione regolare destra

Se nell'esempio precedente avessimo preso la moltiplicazione a destra $(g, h) \mapsto hg$ allora la priprietà (i) continuava a valere in quanto $(1_G) \cdot h = h 1_G = h$, ma per quanto riguarda la proprietà (ii) $(g_1 g_2) \cdot h = h g_1 g_2 \neq h g_2 g_1 = g_1 \cdot (g_2 \cdot h)$. Quindi la funzione $(g, h) \mapsto hg$ non è una azione. Per ottenere un'azione con una moltiplicazione a destra occorre definire un'azione come:

$$\forall\, g, h \in G \quad (g, h) \longmapsto hg^{-1} \qquad \text{(Prodotto a destra per } g^{-1})$$

[1] Indicando con il punto $\cdot$ l'azione tra elementi ed omettendolo per la moltiplicazione in G.

Con questa definizione si ha che (i) $1_G \cdot h = h1_G^{-1} = h$ e (ii) $(g_1g_2) \cdot h = h(g_1g_2)^{-1} = hg_2^{-1}g_1^{-1} = g_1 \cdot (g_2 \cdot h)$. In questo modo è definito l'omomorfismo $\sigma : G \to S_G$ che opera associando ad ogni $g \in G$ l'applicazione $\sigma_g : G \to G$ data dal prodotto a destra per g^{-1}. Il nucleo $\ker \sigma$ è dato da tutti quegli elementi $g \in G$ per cui $\sigma(g) = 1_{S_G} = \mathrm{id}_G$, cioè dagli elementi g tali che $\forall\, h \in G :\ hg^{-1} = h$, in particolare per $h = 1_G$ si ha $g^{-1} = 1_G$. Quindi $\ker \sigma = \{\, 1_G \}$ e σ è fedele. Inoltre opera transitivamente su G in quanto dati $x, y \in G$ si ha che, ponendo $g := y^{-1}x,\ \ x \cdot g = x(y^{-1}x)^{-1} = xx^{-1}y = y$. In questo caso si parla quindi di *rappresentazione regolare destra*.

4.6.3 Esempio: azione per coniugio

Si consideri l'azione $G \times G \to G$ definita da

$$\forall\, g, h \in G \quad (g, h) \longmapsto ghg^{-1} \qquad \text{(Coniugato mediante } g\text{)}$$

È un'azione in quanto vale (i) perché $1_G \cdot h = 1_G h 1_G^{-1} = h$ e (ii) perché $(ab) \cdot h = (ab)h(ab)^{-1} = (ab)h(b^{-1}a^{-1}) = a(bhb^{-1})a^{-1} = a \cdot (b \cdot h)$. Allora è definito l'omomorfismo $\sigma : G \to S_G$ che opera associando ad ogni $g \in G$ l'applicazione $\sigma_g : G \to G$ data dal coniugato mediante g: ghg^{-1}. Tale applicazione può essere vista como composizione di una moltiplicazione a destra per g^{-1} e di una moltiplicazione a sinistra per g. Si usa chiamare l'applicazione coniugio σ_g con il simbolo Int_g. Int_g è un morfismo (come mostrato nel lemma 4.27) biettivo di G in G e quindi è un automorfismo di G: $\mathrm{Int}_g \in \mathrm{Aut}(G)$. Si può verificare direttamente che $\forall\, g \in G,\ \mathrm{Int}(g) = \mathrm{Int}_g$ conserva il prodotto in quanto:

$$\mathrm{Int}_g(h_1h_2) = g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = \mathrm{Int}_g(h_1)\mathrm{Int}_g(h_2)$$

Quindi indicando con Int l'applicazione σ descritta nel lemma 4.27 si può dire che Int è un'applicazione da G in nell'insieme degli automorfismi $\mathrm{Aut}(G)$ di G.
Quale è il suo nucleo? Si ha:

$$\ker \mathrm{Int} = \{\, g \in G :\ h = ghg^{-1}\ \forall\, h \in G \,\} = \{\, g \in G :\ hg = gh\ \forall\, h \in G \,\} = Z(G)$$

Per il teorema di omomorfismo si ha quindi che:

$$G/(\ker \mathrm{Int}) = G/Z(G) \backsimeq \mathrm{Int}(G)$$

Il concetto di coniugato può essere ampliato al caso di gruppi.

Definizione 4.17 *Sia G un gruppo. Si dice che $h_1, h_2 \in G$ sono coniugati se esiste $g \in G$ tale che $h_1 = \mathrm{Int}_g(h_2)$. Si dice che due sottogruppi H_1 ed H_2 di G sono coniugati se esiste $g \in G$ tale che $H_1 = \mathrm{Int}_g(H_2)$ (ovvero se $H_1 = gH_2g^{-1}$).*

Data l'azione di coniugio e dato un elemento $h \in G$ l'orbita di h è data da $Gh = \{\, g \cdot h = ghg^{-1} :\ \forall\, g \in G \,\}$ e viene detta *classe di coniugio* contenente h. Lo stabilizzatore di h è dato da:

$$G_h = \{\, g \in G :\ ghg^{-1} = h \,\} = \{\, g \in G :\ gh = hg \,\} = C_G(h)$$

cioè è il *centralizzante* di h in G (insieme degli elementi di G che commutano con h). Quanti sono i coniugati distinti di G? Per la proposizione 4.29 si ha che $|Gh| = (G : C_G(h))$ e quindi sono tanti quanti i laterali del centralizzante. In particolare si ha che $|Gh| = 1$ se e solo se $ghg^{-1} = h\ \forall\, g \in G$ se e solo se $h \in Z(G)$.
La seguente proposizione è l'equazione delle orbite vista nel caso in cui l'azione è il coniugio (e le orbite le classi di coniugio).

Proposizione 4.32 *Sia G un gruppo finito e sia $\{ x_1, \ldots, x_s \}$ un sistema completo di rappresentanti per le classi di coniugio di elementi di $G \setminus Z(G)$. Allora:*

$$|G| = |Z(G)| + \sum_{i=1}^{s} \frac{|G|}{|G_{x_i}|} = |Z(G)| + \sum_{i=1}^{s} \frac{|G|}{|C_G(x_i)|}$$

Trattiamo ora *l'azione per coniugio sui sottogruppi di un gruppo G*. Sia X l'insieme di tutti i sottogruppi di G e sia l'azione $G \times X \to X$ definita da:

$$\forall\, g \in G;\ \forall\, H \leq G;\ \ (g, H) \longmapsto gHg^{-1}$$

Indichiamo l'orbita di H in G con $G(H)$. L'orbita di un sottogruppo H è detta *classe di coniugio* di H ed è l'insieme dei gruppi coniugati di H. Quanti diversi coniugati di un gruppo ci sono? Si ha:

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

Lo stabilizzante di H in G viene detto *normalizzante* e si indica con $N_G(H)$. Il termine normalizzante deriva dal fatto che $gHg^{-1} = H \iff gH = Hg$ e quindi $N_G(H)$ è il più grande insieme degli elementi di G in cui H è normale.

4.7 Teoremi di Sylow

Il seguente lemma caratterizza i sottogruppi di gruppi ciclici.

Lemma 4.33 (Sottogruppi ciclici)
(i) *Ogni sottogruppo di un gruppo ciclico è ciclico.*
(ii) *Sia G un gruppo ciclico finito di ordine n. Allora per ogni divisore $d > 0$ di n esiste ed è unico un sottogruppo di G di ordine d.*

***D**imostrazione.* (i) Sia $G = \langle a \rangle \leq G$ e $H \leq G$. Allora H è ciclico. Infatti se $H = \{ 1_G \}$ la tesi è ovvia. Se $H \neq \{ 1_G \}$ allora esiste $r > 0$ tale che $a^r \in H$. L'insieme degli esponenti positivi tali che $a^m \in H$ ha minimo per l'assioma del buon ordinamento. Sia t tale minimo. Sia ora $a^m \in H$. Allora dividendo m per t si ha $m = qt + r$ con $0 \leq r < t$. Segue che $a^m = (a^t)^q a^r \implies a^r = (a^t)^{-q} a^m \in H$ in quanto $a^t, a^m \in H$. Per la minimalità di t non può che essere $r = 0$. Si conclude che $a^m = (a^t)^q \in \langle a^t \rangle$ e quindi $H = \langle a^t \rangle$ per la proposizione 3.9 pagina 30.
(ii) Sia $G = \langle a \rangle$ ciclico con $|G| = n$ e sia d un divisore di $n = kd$. Proviamo che $\langle a^k \rangle$ è un sottogruppo di ordine d. Per la 3.12 pagina 32 si ha che:

$$o(a^k) = n/\mathrm{MCD}(k, n) = n/k = d$$

Dunque $|\langle a^k \rangle| = d$. Proviamo ora che è l'unico sottogruppo di ordine d. Sia K un altro sottogruppo di ordine d. Per il punto (i) K è ciclico: $K = \langle a^t \rangle$. Segue che:

$$o(a^t) = n/\mathrm{MCD}(t, n) \implies n = \mathrm{MCD}(t, n) \cdot d \implies \mathrm{MCD}(t, n) = k$$

In particolare $k \mid t$ e quindi $a^t = a^{kq}$ per qualche q. Allora $a^t = a^{kq} = (a^k)^q \in \langle a^k \rangle$. Essendo quindi il generatore a^t contenuto in $\langle a^k \rangle$ si ha che $K \subseteq \langle a^k \rangle$, ma siccome hanno lo stesso ordine devono necessariamente coincidere. ∎

Il teorema seguente è il principale risultato di questo paragrafo. La versione della dimostrazione qui presentata segue la dimostrazione di H. Wielandt che alcuni fanno risalire A. Capelli.

Proposizione 4.34 *Sia G un gruppo finito di ordine n e sia p^a una potenza qualsiasi del numero primo p tale che p^a divide n (cioè tale che $n = p^a m$). Sia $N(p^a)$ il numero dei sottogruppi di G di ordine p^a. Allora:*

$$N(p^a) \equiv 1 \ _{(p)}$$

In particolare $N(p^a) \geq 1$.

***D**imostrazione.* Sia X l'insieme di tutti i *sottoinsiemi* di G di cardinalità p^a:

$$X = \{ S \subseteq G : \ |S| = p^a \}$$

Proviamo che in X c'è un numero di *sottogruppi* congruo a 1 modulo p. X è formato da tutti i sottoinsiemi di cardinalità p^a di G (che ha cardinalità $n = p^a m$).

$$\text{Si ha dunque:} \quad |X| = \binom{n}{p^a} = \binom{p^a m}{p^a}.$$

Consideriamo ora l'azione di G sull'insieme X definita da:

$$\forall\, g \in G, \forall\, S \in X; \quad (g, S) \longmapsto gS = \{ gs : \ \forall\, s \in S \}$$

Cioè l'azione che ad ogni $g \in G$ e ad ogni $S \in X$ associa il sottoinsieme di G dato dal prodotto gS. Sia $\{ S_i \}$ un sistema completo di rappresentanti per le orbite di G su X (che saranno in numero finito). Le orbite formano una partizione di X e dunque, indicando con GS_i l'orbita contenente S_i si ha:

$$|X| = \sum_i |GS_i| \tag{1}$$

Indicando con G_{S_i} lo stabilizzatore di S_i in G si ha che $G_{S_i}S_i = S_i$ (i.e. ogni elemento dello stabilizzatore fissa l'elemento S_i di X). È possibile allora pensare ad S_i come unione di laterali destri del sottogruppo G_{S_i}. Infatti si ha:

$$S_i = \{ s_{i1}, \ldots, s_{ir_i} \} = G_{S_i}S_i \quad \text{e quindi:}$$
$$S_i = \bigcup_{j=1}^{\bullet\, r_i} G_{S_i}s_{ij} \qquad (\text{con } s_{ij} \in S_i) \tag{2}$$

dove r_i è il numero di laterali che fanno l'unione. Ogni laterale ha cardinalità pari a $|G_{S_i}|$ e quindi, essendoci r_i laterali [1]:

$$p^a = |S_i| = r_i|G_{S_i}| \implies |G_{S_i}| = p^{b_i} \qquad (\text{per qualche } b_i \leq a) \tag{3}$$

Se $b_i < a$, allora per la proposizione 4.29 si ha:

$$|GS_i| = \frac{|G|}{|G_{S_i}|} = \frac{n}{p^b} = p^{a-b_i}m \equiv 0 \ _{(pm)}$$

Se $b_i = a$ allora si ha:

$$|GS_i| = \frac{|G|}{|G_{S_i}|} = \frac{p^a m}{p^a} = m \not\equiv 0 \ _{(pm)}$$

Quindi andando a studiare a cosa è congrua la quantità $|X|$ modulo pm possiamo eliminare dalla (1) tutti i termini congrui a 0 modulo m ottenendo:

$$|X| = \binom{p^a m}{p^a} \equiv \sum_{|GS_i|=m} |GS_i| \ _{(pm)} \tag{4}$$

Se $b_i = a$ e quindi se $|GS_i| = m$ allora dalla (3) si legge che $|S_i| = |G_{S_i}| = p^a$ e quindi che $r_i = 1$. Allora per la (2) S_i coincide con un unico laterale destro. Vi è cioè un unico $s_i \in S_i$ tale che $S_i = G_{S_i}s_i$. Moltiplicando a sinistra per s_i^{-1} si ottiene quindi che:

$$B_i := s_i^{-1}S_i = s_i^{-1}G_{S_i}s_i$$

È il coniugato mediante $s_i \in G$ di un sottogruppo [2] e quindi è un sottogruppo di G. B_i ha ordine p^a e sta nell'orbita GS_i. In particolare i laterali sinistri gB_i descrivono tutta l'orbita GS_i. Quindi data un orbita di lunghezza m ad essa corrisponde in modo univoco un sottogruppo B_i di G.

[1] E ricordando che se $ab = p^a$ allora per il *teorema fondamentale dell'aritmetica* devono essere opportune potenze di p, essendo p un numero primo.

[2] Dello stabilizzatore che è un sottogruppo normale per quanto osservato a pagina 50.

Inversamente, ad ogni sottogruppo U di G di ordine p^a è associata una G-orbita su X di lunghezza m definita da:

$$O := \{\, gU : \forall\, g \in G \,\} \qquad \text{(laterali sinistri di } U\text{)}$$

Per il teorema di Lagrange 4.4 essendo $|G| = p^a m$ e U un sottogruppo di ordine p^a si ha che il quoziente $p^a m/p^a = m$ è il numero dei possibili laterali di U in G. Quindi l'orbita O che corrisponde al sottogruppo U ha lunghezza m. Mostriamo che per U diversi si ottengono O diverse. Se $U_1 \neq U_2$ sono due sottogruppi di G di ordine p^a allora le orbite $O_1 = \{\, gU_1 \,\}$ e $O_2 = \{\, gU_2 \,\}$ sono distinte. Infatti se per assurdo così non fosse sarebbe $U_1 = gU_2$ per un opportuno $g \in G$. In particolare $1_G = gu_2$ per qualche $u_2 \in U_2$. Segue che $g = u_2^{-1} \in U_2$ e quindi che $U_1 = gU_2 = U_2$

Quindi abbiamo stablilito che esiste una bijezione tra le orbite GS_i di lunghezza m e i sottogruppi di G di ordine p^a. Segue che ci sono tanti sottogruppi di ordine p^a quante orbite di lunghezza m. Quindi dalla (4) otteniamo [3] :

$$|X| = \binom{p^a m}{p^a} \equiv m \cdot N(p^a) \pmod{pm} \tag{5}$$

Questa condizione vale in generale per qualsiasi gruppo finito G. In particolare deve valere se G è un gruppo ciclico. Per il lemma 4.33 in un gruppo ciclico per ogni divisore dell'ordine esiste uno ed un solo sottogruppo di quell'ordine. Quindi $N(p^a) = 1$.
Si ottiene quindi la seguente relazione (che è una condizione necessaria):

$$|X| = \binom{p^a m}{p^a} \equiv m \pmod{pm}$$

Segue che (per 2.8): $m \equiv m \cdot N(p^a) \pmod{pm} \implies N(p^a) \equiv 1 \pmod{p}$. ■

Definizione 4.18 *Sia G un gruppo finito e p un numero primo.*
(i) *G si dice un p-gruppo se l'ordine di G è una potenza di p.*
(ii) *Un sottogruppo $H \subseteq G$ si dice un p-sottogruppo di Sylow se H è un p-gruppo e se l'ordine di H è la massima potenza di p. Cioè se $|H| = p^a$ e $|G| = p^a n$ con $p \nmid n$.*
Si denota con $\mathrm{Syl}_p(G)$ l'insieme dei p-sottogruppi di Sylow di G.

Corollari della proposizione precedente sono i seguenti.

Corollario 4.35 (Primo teorema di Sylow)
Se p è un primo che divide $|G|$, G contiene dei p-sottogruppi di Sylow e il numero di tali sottogruppi è congruo a 1 modulo p.

***D**imostrazione.* È un caso particolare di 4.34. ■

Corollario 4.36 (Teorema di Cauchy)
Se p è un divisore primo dell'ordine di un gruppo, G contiene elementi di periodo p.

***D**imostrazione.* Per la proposizione 4.34 se $p = p^1$ divide l'ordine di G allora c'è almeno un sottogruppo di G di ordine p. Per il corollario 4.24 tale gruppo è ciclico. ■

[3] La somma nella (4) è pari al numero di orbite di lunghezza m moltiplicato per m. Per quanto visto il numero di orbite è esattamente $N(p^a)$.

Teorema 4.37 (Secondo teorema di Sylow)
Sia G un gruppo finito e p un numero primo. Allora:
(i) *Se P è un p-sottogruppo di Sylow di G e U è un sottogruppo di ordine una potenza di p, allora $\exists\, g \in G$ tale che $U \subseteq gPg^{-1}$.*
(ii) *I p-sottogruppi di Sylow di G formano una classe di coniugio di sottogruppi di G. In particolare:*

$$N(p^k) = \frac{|G|}{|N_G(P)|} \qquad (con\ |G| = p^k m\ \ e\ \ p \nmid m\ )$$

Cioè il numero dei p-sottogruppi di Sylow divide l'ordine del gruppo ed il quoziente è la cardinalità del normalizzante di uno dei p-sottogruppi.

***D**imostrazione.* (i) Si ha che $|G| = p^k m$ con $p \nmid m$, $|P| = p^k$ e $|U| = p^a$ con $a \leq k$. Indichiamo con $G\backslash P$ l'insieme dei laterali sinistri di P in G. Consideriamo l'azione $U \times G\backslash P \to G\backslash P$ di U su $X = G\backslash P$ definita da:

$$(u, gP) \longmapsto (ug)P$$

Essendo la lunghezza dell'orbita di $gP \in X$ pari all'indice dello stabilizzante U_{gP} (4.29) si ha che:

$$|UgP| = |U|/|U_{gP}| \implies |UgP| \cdot |U_{gP}| = |U| = p^a$$

Quindi la lunghezza di ogni orbita, dovendo dividere $|U|$, deve essere necessariamente una potenza di p. Per il teorema di Lagrange (4.4) applicato al sottogruppo P si ha:

$$|P| \cdot |G\backslash P| = |G| \implies |G\backslash P| = \frac{|G|}{|P|} = m \implies p \nmid m = |G\backslash P|$$

Le orbite non possono però essere tutte di lunghezza p^b con $b > 1$ perché altrimenti dall'equazione delle orbite (4.30):

$$|G\backslash P| = \sum_{i=1}^{r} |UgP| = \sum_{i=1}^{r} p^{b_i} = \sum_{i=1}^{r} p \cdot p^{b_i - 1} = p \sum_{i=1}^{r} p^{b_i - 1}$$

si avrebbe che p divide $|G\backslash P|$. Quindi almeno un'orbita deve avere lunghezza pari a $p^0 = 1$. Allora deve esistere un elemento gP tale che:

$$\forall\, u \in U, \quad ugP = gP \qquad \text{cioè...} \qquad \forall\, u \in U, \quad ug \in gP$$

Ovvero $u \in gPg^{-1}$. Si conclude che $U \subseteq gPg^{-1}$.
(ii) Per il punto precedente, se U e P sono due p-gruppi di Sylow allora (essendo in particolare U un p-gruppo) si ha che $U \subseteq gPg^{-1}$ per un opportuno $g \in G$. Allora, essendo il coniugato di un gruppo di Sylow un gruppo di Sylow, si ha che $U = gPg^{-1}$ (perché hanno lo stesso ordine). Quindi due p-gruppi di Sylow sono sempre coniugati tra loro. Sia quindi X l'insieme dei p-sottogruppi di Sylow in G e sia $S \in X$. Lo stabilizzante di $S \in X$ si indica con $N_G(S)$ ed è detto *normalizzante*. Essendo tutti i p-sottogruppi di Sylow coniugati tra loro, l'azione di coniugio

$$G \times X \to X, \qquad (g, P) \longmapsto gPg^{-1}$$

è transitiva. Essendoci quindi una unica orbita questa viene a coincidere con X. Quindi (essendo lunghezza orbita = indice stabilizzante) si ha che:

$$|X| = (G : N_G(S)) = |G|/|N_G(S)|$$

E questo conclude la dimostrazione. ■

OSSERVAZIONE Ricordiamo che un gruppo G si dice *semplice* se gli unici sottogruppi *normali* [4] sono $\{1_G\}$ e G. Si osservi inoltre che se in un gruppo G vi è un solo p-sottogruppo di Sylow S allora in virtù del fatto che i p-sottogruppi di Sylow sono tutti coniugati si ha che ogni coniugato di S deve coincidere con S (che è l'unico elemento della classe di coniugio). Quindi la condizione

$$\forall\, g \in G,\ \ gSg^{-1} = S \iff gS = Sg$$

equivale alla normalità di S in G.

Proposizione 4.38 *Sia G un gruppo finito.*
Sia P un p-sottogruppo di Sylow di G ($P \in \mathrm{Syl}_p(G)$) e $N \trianglelefteq G$. Allora:
(i) $P \cap N \in \mathrm{Syl}_p(N)$ *($P \cap N$ è un p-sottogruppo di Sylow in N)*
(ii) $(PN)/N \in \mathrm{Syl}_p(G/N)$

***D**imostrazione.* **Da completare.** ∎

Proposizione 4.39 *Siano p, q due numeri primi con $p < q$ e $p \nmid (q-1)$.*
Allora ogni gruppo di ordine pq è ciclico.

***D**imostrazione.* Sia G un gruppo di ordine pq. Siano n_p ed n_q rispettivamente il numero dei p-sottogruppi di Sylow e il numero dei q-sottogruppi di Sylow:

$$n_p := |\mathrm{Syl}_p(G)| \qquad n_q := |\mathrm{Syl}_q(G)|$$

Mostriamo che *esistono unici $P \in \mathrm{Syl}_p(G)$ e $Q \in \mathrm{Syl}_q(G)$ sottogruppi (normali, cilcici, abeliani) di Sylow e che $G = PQ$*. Per il secondo teorema di Sylow n_p ed n_q devono dividere l'ordine del gruppo G. Quindi $n_p, n_q \in \{1, p, q\}$. Per il primo teorema di Sylow deve essere $n_p \equiv 1\ _{(p)}$ che equivale a dire $p \mid (n_p - 1)$. Procedendo in modo analogo con n_q si ottiene $q \mid (n_q - 1)$.
- n_p non può essere uguale a p perché $p \nmid (p-1)$.
- n_p non può essere uguale a q perché $p \nmid (q-1)$ per ipotesi.
Segue che $n_p = 1$ cioè che esiste un unico p-sottogruppo di Sylow di G. Essendo l'unico è un sottogruppo normale in G e ha ordine primo. Se un sottogruppo ha ordine un numero primo allora è ciclico (4.6), e quindi abeliano (3.8).
- n_q non può essere uguale a q perché $q \nmid (q-1)$.
- n_q non può essere pari a p perché altrimenti $q \mid (p-1) \implies q \leq p-1$ ma $p < q$.
Allora $n_q = 1$ e quindi esiste uno ed un solo q-sottogruppo di Sylow, normale, ciclico ed abeliano. Siano quindi $P \in \mathrm{Syl}_p(G)$ e $Q \in \mathrm{Syl}_q(G)$. Consideriamo il prodotto $PQ = \{hk \in G :\ \forall\, h \in P,\ \forall\, k \in Q\}$. Per 4.12 si ha:

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|}$$

Essendo l'intersezione di due sottogruppi un gruppo (3.7) per il teorema di Lagrange $|P \cap Q|$ deve dividere p in quanto $P \cap Q \leq P$. In modo analogo $|P \cap Q|$ deve dividere q. Allora deve dividere $\mathrm{MCD}(p, q) = 1$. Quindi si ha che $|P \cap Q| = 1$.

$$|G| = |PQ| = |P| \cdot |Q| \implies G = PQ$$

Mostriamo che G *è abeliano*. Siano $x \in P,\ y \in Q$. Consideriamo $xyx^{-1}y^{-1}$. Essendo $Q \trianglelefteq G$ si ha $xyx^{-1} \in Q$. Essendo $y^{-1} \in Q$, $xyx^{-1}y^{-1} \in Q$. D'altra parte $yx^{-1}y^{-1} \in P$ perché $P \trianglelefteq G$ e dunque $xyx^{-1}y^{-1} \in P$. Quindi $xyx^{-1}y^{-1} \in P \cap Q = \{1_G\}$. Segue che $xyx^{-1}y^{-1} = 1_G \implies xy = yx$ e quindi[5] che G é abeliano.

[4] H è normale se $\forall\, g \in G,\ \ gH = Hg$.

[5] Se $a, b \in G$ allora (essendo $G = PQ$) si ha $a = x_1y_1,\ b = x_2y_2$ con $x_i \in P,\ y_i \in Q$. Allora per quanto visto $ab = x_1y_1x_2y_2 = x_1x_2y_1y_2 = x_2x_1y_2y_1 = x_2y_2x_1y_1 = ba$.

Mostriamo che G *è ciclico*. Essendo P, Q ciclici si ha $P = \langle g_1 \rangle$, $Q = \langle g_2 \rangle$ con $o(g_1) = p$, $o(g_2) = q$. Avendo provato che G è abeliano possiamo usare il lemma 3.13 concludendo che

$$o(g_1 g_2) = o(g_1)o(g_2) = pq = |G|$$

Quindi G è ciclico generato da $g_1 g_2$. ■

ESEMPI

1. Sia G un gruppo tale che $|G| = 30$. Indichiamo con $N(p^k) = |\mathrm{Syl}_p(G)|$.
   Per i teoremi di Sylow deve essere $N(p^k) \mid 30 = 2 \cdot 3 \cdot 5$ e $N(p^k) \equiv 1_{(p)}$.
   Quindi $N(5) \in \{1, 6\}$ e $N(3) \in \{1, 10\}$.

   - Se $N(3) = 1$ allora esiste un unico sottogruppo normale $P \trianglelefteq G$ di ordine 3. Tale sottogruppo ha ordine primo ed è quindi ciclico (e dunque abeliano).
   - Se invece $N(3) = 10$ allora esistono $P_1, \ldots, P_{10} \in \mathrm{Syl}_3(G)$. L'intersezione $P_i \cap P_j : i \neq j$ è un sottogruppo di P_i e per il teorema di Lagrange il suo ordine deve dividere $|P_i| = 3$. Quindi, essendo $P_i \neq P_j$, deve essere $|P_i \cap P_j| = 1$ cioè $P_i \cap P_j = \{1_G\}$. Quindi per ogni $i = 1, \ldots 10$ si ha un gruppo $P_i = \{1_G, x_{i1}, x_{i2}\}$ in cui $o(x_{i1}) = o(x_{i2}) = 3$. Ci sono quindi 10 gruppi con intersezione banale ed ogni gruppo ha due elementi di ordine 3, per un totale di 20 elementi di ordine 3. Mancano 9 elementi diversi dall'unità, con ordine diverso da 3.
   - Se $N(5) = 1$ allora esiste un unico sottogruppo normale $Q \trianglelefteq G$ di ordine 5.
   - Se $N(5) = 6$ allora esistono $Q_1, \ldots, Q_6 \in \mathrm{Syl}_5(G)$. L'intersezione $Q_i \cap Q_j$ è banale se $i \neq j$. Ogni elemento di Q_i diverso da 1_G ha ordine 5. Ci sono quindi 6 gruppi ed ogni gruppo ha 4 elementi di ordine 5, per un totale di 24 elementi di ordine 5.

   Essendoci in totale 30 elementi l'ipotesi $N(3) = 10 \wedge N(5) = 6$ è da scartare. Allora o $N(3) = 1$ oppure $N(5) = 1$. In ogni caso si trova un sottogruppo normale non banale. Si conclude che *un gruppo di ordine* 30 *non è semplice.*

2. Sia G un gruppo tale che $|G| = 15 = 3 \cdot 5$. Allora si ha che per $p = 3$ e $q = 5$ il gruppo soddisfa le ipotesi del teorema precedente in quanto $3 \nmid 4$. Quindi G è un gruppo ciclico (e quindi abeliano).

3. Sia G un gruppo di ordine $21 = 3 \cdot 7$. G non soddisfa le ipotesi del teorema precedente in quanto $3 \mid (7 - 1)$. Quindi procediamo in modo diretto. Per il teorema di Lagrange un sottogruppo può avere ordine $1, 3, 7, 21$. I sottogruppi di ordine 1 e 21 sono soltanto quelli banali. I sottogruppi di ordine 3 e 7 corrispondono alla massima potenza di 3 e di 7 che compare nell'ordine di G e sono quindi dei p-Sylow. Si ha $N(3) \in \{1, 7\}$, $n_7 \in \{1\}$. Quindi esiste un solo 7-sottogruppo di Sylow $P \trianglelefteq G$, ciclico ed abeliano. In particolare G non è semplice.

4. *Se G è un gruppo tale che $|G| = pq$ con p, q primi distinti allora G non è semplice.*
   A meno di scambiare p e q possiamo supporre $p > q$. Allora per i teoremi si Sylow $N(p) \in \{1, q\}$. Se per assurdo $N(p) = q$ allora $q \equiv 1_{(p)} \implies q = mp + 1$ con $m > 0$. Segue che $q > p$, assurdo. Quindi esiste un unico p-sottogruppo di Sylow di G. Per quanto riguarda i q-sottogruppi non possiamo concludere nulla in generale. Infatti $p \equiv 1_{(p)} \implies p = mq + 1$ non porta ad alcuna contraddizione.

5. *Se G è un gruppo abeliano avente come ordine il prodotto di numeri primi distinti allora G è ciclico.* Sia $|G| = p_1 \dots p_s$ la fattorizzazione (unica) in fattori primi dell'ordine del gruppo G. Procediamo per induzione sul numero di fattori s. Se $s = 1$ allora G è ovviamente ciclico. Sia ora la tesi vera fino ad un certo s (escluso) e proviamola per s. Per il teorema di Cauchy esiste un elemento x di ordine p_s. Allora $H := \langle x \rangle$ è un sottogruppo normale di G. Se consideriamo il gruppo quoziente G/H si ha, per il teorema di Lagrange, che $|G/H| = |G|/|H| = p_1 \dots p_{s-1}$. Quindi possiamo applicare l'ipotesi induttiva[6] su G/H e concludere che è ciclico. Sia dunque Hy un generatore.

[6] In quanto il quoziente di un gruppo commutativo è un gruppo commutativo (proprietà equazionale ereditata sulle operazioni definite sul quoziente).

5 Anelli, corpi, campi

5.1 Anelli, domini: definizioni ed esempi

Definizione 5.1 *Sia A un insieme non vuoto su cui sono definite due operazioni binarie $+$ e $\cdot$. Si dice che $(A, +, \cdot)$ è un anello se:*
(i) *$(A, +)$ è un gruppo abeliano.*
(ii) *$(A, \cdot)$ è un monoide.*
(iii) *$\forall\, a, b, c \in A$ si ha (proprietà distributive):*

$$a \cdot (b + c) = ab + ac$$
$$(a + b) \cdot c = ac + bc$$

Un anello si dice commutativo se il prodotto è commutativo.

NOTAZIONE Quando parleremo di anello in generale assumeremo che stiamo parlando di un anello *non* commutativo. Si usa indicare le operazioni assumendo implicitamente che l'operazione di prodotto abbia la priorità rispetto a quella di somma. Pertanto una scrittura come $a \cdot b + c$ sarà da intendersi come $(a \cdot b) + c$. L'unità del gruppo $(A, +)$ viene detta *zero dell'anello* e si indica con 0_A oppure con $\underline{0}$. L'unità del monoide $(A, \cdot)$ viene detta *unità dell'anello* e si indica con 1_A.

ESEMPI

1. $(\mathbb{Z}, +, \cdot)$ è l'anello degli interi. Anche $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ e $(\mathbb{C}, +, \cdot)$ sono anelli.
2. Per $n > 1$ l'insieme $(\mathbb{Z}/n\mathbb{Z})$ con la somma e il prodotto definite sulle classi resto modulo n è un anello finito (campo se n è primo).
3. Se A è un anello è possibile definire l'insieme $\mathrm{Mat}(n, A)$ come l'insieme delle matrici quadrate di ordine n con elementi in A. Definendo la somma di matrici componente per componente e il tradizionale prodotto righe per colonne si ha che $(\mathrm{Mat}(n, A), +, \cdot)$ è un anello non commutativo (anche se A lo è). In realtà è altamente non abeliano in quanto il centro è costituito dalle sole matrici scalari.

Definizione 5.2 *Un sottoinsieme B di un anello A si dice sottoanello di A se:*
(i) *$(B, +)$ è un sottogruppo di $(A, +)$.*
(ii) *$(B, \cdot)$ è un sottomonoide del monoide $(A, \cdot)$.*
Se B è un sottoanello di A si scrive $B \leq A$.

Definizione 5.3 *Siano A e B anelli.*
Una applicazione $F : A \to B$ si dice (omo)morfismo di anelli se:
(i) *$F(x + y) = F(x) + F(y)$ (morfismo del gruppo abeliano $(A, +)$)*
(ii) *$F(xy) = F(x)F(y)$ (morfismo del monoide $(A, \cdot)$)*
(iii) *$F(1_A) = 1_B$*
Si usa indicare con epi-mono-iso la suriettività, iniettività, bijettività.
Due anelli A e B si dicono isomorfi se esiste un isomorfismo $A \to B$.

OSSERVAZIONE Si osservi che la condizione $F(1_A) = 1_B$, diversamente dal caso dei morfismi di gruppi, non è una condizione ridondante in quanto $(A, \cdot)$ *non* è un gruppo e quindi non vale la legge di cancellazione. Non è possibile quindi condurre una dimostrazione simile a quella del lemma 4.14 a pagina 42.

Valgono le seguenti proprietà elementari.

Lemma 5.1 *Per ogni a, b, c in un anello A e per ogni $n \in \mathbb{Z}$ si ha:*
(i) $0_A \cdot a = a \cdot 0_A = 0_A$. *(prop. zero)*
(ii) $(-a)b = a(-b) = -(ab)$. *(regola dei segni)*
(iii) $(na)b = a(nb) = n(ab)$. *(prop. multiplo)*

***D**imostrazione.* (i) Usando la proprietà distributiva e la legge di cancellazione[1]:
$a^2 = a \cdot a = a(a + 0_A) = a^2 + (a \cdot 0_A) \implies a \cdot 0_A = 0_A$.
In modo analogo dalla destra segue che $0_A \cdot a = 0_A$
(ii) Per il primo punto $0_A = a \cdot 0_A = a(b+(-b)) = ab+a(-b)$ e quindi $a(-b)$ funziona da opposto [2] di ab. Segue che $a(-b) = -ab$. In modo analogo dalla sinistra.
(iii) Sia $n \geq 0$. Procediamo per induzione su n. Per $n = 0$ è il punto (i). Supposta la tesi vera per $n-1$ si ha $(na)b = ((n-1)a+a)b = ((n-1)a)b+ab = (n-1)(ab)+(ab) = n(ab)$. In modo analogo dall'altro lato. Se invece $n < 0$ allora basta passare a $-n$ e usare quanto visto. ∎

Definizione 5.4 *Sia A un anello. $a \in A$, $a \neq 0_A$ si dice divisore dello zero se esiste $b \in A$, $b \neq 0_A$ tale che $ab = 0_A$ oppure $ba = 0_A$.*

Osservazione Un anello è privo di divisori dello zero se e solo se $A^* = A \setminus \{0_A\}$ è chiuso rispetto al prodotto (i.e. il prodotto di due elementi diversi dallo zero è diverso dallo zero).

Esempi

1. Conseguenza degli assiomi dei numeri interi è che $(\mathbb{Z}, +, \cdot)$ è privo di divisori dello zero.
2. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ è privo di divisori dello zero se e solo se n è primo. Infatti per ogni $[r]_n, [s]_n \in \mathbb{Z}/n\mathbb{Z}$ possiamo supporre $0 \leq r, s < n$ (prendendo i rappresentanti principali). Segue che:

   $$[r]_n \cdot [s]_n = [0]_n \implies [rs]_n = [0]_n \implies rs \equiv 0 \ _{(n)}$$

   Quindi deve essere $n \mid rs$. Allora, essendo n primo, per definizione si ha che $n \mid r$ o $n \mid s$. In altre parole $[r]_n = [0]_n$ oppure $[s]_n = [0]_n$. In particolare abbiamo verificato che *la proprietà di avere divisori dello zero non passa al quoziente.*
3. Se A è un anello commutativo l'anello $(\mathrm{Mat}(n, A), +, \cdot)$ per $n > 1$ ha sempre divisori dello zero indipendentemente dal fatto che A li abbia o no. Infatti se si pensa al prodotto di matrici elementari si ha [3] :

   $$E_{ij} \cdot E_{kl} = \delta_{ik} E_{il}$$

   In particolare ogni volta che $j \neq k$ le matrici date sono divisori dello zero.

Il fatto di avere o no divisori dello zero ha influenza sulle "regole di calcolo", come mostra la seguente proposizione.

---

[1] Nel gruppo additivo $(A, +)$.
[2] Ed è quindi l'unico opposto per la proposizione 1.9 a pagina 12.
[3] Indicando con δ_{ij} il simbolo di Kronecker ($\delta_{ij} = 0$ se $i = j$; $\delta_{ij} = 1$ se $i \neq j$) e con E_{ij} la matrice avente $a_{ij} = 1$ e zero altrove.

Proposizione 5.2 *Un anello A è privo di divisori dello zero se e solo se valgono in A le leggi di cancellazione rispetto al prodotto. Cioè se e solo se per ogni $a \in A$, $a \neq 0_A$ e per ogni $x, y \in A$:*

$$ax = ay \implies x = y \qquad e \qquad xa = ya \implies x = y$$

***D**imostrazione.* Supponiamo che A sia privo di divisori dello zero. Allora:
$a \neq 0_A$, $ax = ay \implies ax - ay = 0_A \implies a(x-y) = 0_A \implies x - y = 0_A \implies x = y$.
In modo analogo dalla destra. Viceversa valgano le leggi di cancellazione. Se $ab = 0_A$ con $a \neq 0_A$ allora $ab = a \cdot 0_A \implies b = 0_A$. Stesso discorso per $ba = 0_A$. ∎

Definizione 5.5 *Un anello D si dice dominio di integrità (o dominio) se:*
(i) *D è commutativo.*
(ii) *D è privo di divisori dello zero.*

Esempi

1. $(\mathbb{Z}, +, \cdot)$ è un dominio di integrità.
2. Un sottoanello di un dominio di integrità è ovviamente un dominio di integrità.

Definizione 5.6 *Sia A un anello e $a \in A$.*
Si dice che a è unitario se è invertibile rispetto al prodotto, cioè se:

$$\exists\, \widetilde{a} \in A \quad tale\ che \quad a\widetilde{a} = \widetilde{a}a = 1_A \qquad (\widetilde{a} = a^{-1})$$

Indicheremo l'insieme degli elementi unitari di A con $\mathcal{U}$.

Lemma 5.3 *L'insieme $\mathcal{U}$ degli elementi unitari di un anello A è un gruppo rispetto al prodotto definito in A.*

***D**imostrazione.* (i) $1_A \in \mathcal{U}$ in quanto $1_A^2 = 1_A$. (ii) Se $a \in \mathcal{U}$ allora ovviamente $a^{-1} \in \mathcal{U}$. (iii) Se $a, b \in \mathcal{U}$ (e quindi esistono a^{-1} e b^{-1} in A) allora $(ab)^{-1} = b^{-1}a^{-1}$ esiste in A in quanto $abb^{-1}a^{-1} = 1_A$ e lo stesso vale a sinistra. ∎

Lemma 5.4 *Un elemento unitario non è divisore dello zero.*

***D**imostrazione.* Se $a \in \mathcal{U}$ (esiste in A l'inverso a^{-1} di a).
Allora $ab = 0_A \implies a^{-1}(ab) = 0_A \implies (a^{-1}a)b = 0_A \implies b = 0$. ∎

Osservazione Attenzione! non vale il viceversa. In $(\mathbb{Z}, +, \cdot)$ gli elementi unitari sono ± 1 ma non ci sono divisori dello zero!

Esempi

1. Quali sono gli elementi unitari nell'anello $\mathbb{Z}/n\mathbb{Z}$? Per quanto osservato a pagina 23 l'elemento $[\,a\,]_n \in \mathcal{U}$ (è invertibile rispetto al prodotto) se e solo se $\mathrm{MCD}(a, n) = 1$. In questo caso si ha quindi che i non unitari sono tutti e soli i divisori dello zero.
2. Se $\mathbb{K}$ è un campo e consideriamo l'anello $\mathrm{Mat}(n, \mathbb{K})$ per $n > 1$ allora gli elementi unitari sono le matrici non singolari. Tutte le matrici diverse dalla matrice nulla avente determinante nullo sono allora divisori dello zero. Infatti se il rango di A è minore di n il sistema omogeneo $A\underline{x} = \underline{0}$ ammette soluzioni non banali. Segue che, se $\underline{x}_0 \in \mathbb{R}^n$ è una soluzione non banale, la matrice:

$$A^* = \left(\begin{array}{c|c|c|c} \underline{x}_0 & \underline{0} & \dots & \underline{0} \end{array} \right)$$

È una matrice non nulla tale per cui $A \cdot A^*$ è la matrice nulla. Il gruppo $\mathcal{U}$ degli elementi unitari si denota con $\mathrm{GL}(n, A)$ ed è dato da:

$$\mathrm{GL}(n, A) = \{\, X \in \mathrm{Mat}(n, A) : \ \det(X) \text{ è unitario in } A. \,\}$$

OSSERVAZIONE Se A e B sono due anelli isomorfi e A è un dominio, allora anche B è un dominio. Infatti sia $f : A \to B$ l'isomorfismo. Se $b_1, b_2 \in B$ allora per la suriettività esistono $a_1, a_2 \in A$ tale che $b_1 = f(a_1)$ e $b_2 = f(a_2)$. Segue che $b_1 b_2 = 0_B \implies f(a_1)f(a_2) = 0_B \implies f(a_1 a_2) = 0_B \implies a_1 a_2 = 0_A$ (in quanto f è iniettivo). Quindi se A è privo di divisori dello zero anche B lo è.

Se $R_1, \ldots, R_n$ sono anelli allora è possibile dare al prodotto cartesiano $R_1 \times \ldots \times R_n$ una struttura di anello nel seguente modo:

Definizione 5.7 *Siano $R_1, \ldots, R_n$ anelli. Definiamo prodotto degli anelli $R_1, \ldots, R_n$ (o somma diretta) l'insieme $R_1 \times \ldots \times R_n$ con le seguenti operazioni:*

$$\textit{Somma:} \quad (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$
$$\textit{Prodotto:} \quad (x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n)$$

È semplice verificare che il prodotto di anelli è un anello e che in tale anello

$$1 = (1_{R_1}, \ldots, 1_{R_n}) \qquad 0 = (0_{R_1}, \ldots, 0_{R_n})$$

OSSERVAZIONE Si osservi che se $R_1, \ldots, R_n$ sono anelli e $n > 1$ allora l'anello prodotto ha sempre divisori dello zero. In particolare se F è un campo allora $F \times F$ non lo è!

5.1.1 Esempio: elementi unitari in $\mathbb{Z}/n\mathbb{Z}$

Proposizione 5.5 *Sia $A = \mathbb{Z}/n\mathbb{Z}$. Allora:*
(i) $0_A \neq [\,a\,]_n \in A$ *è unitario se e solo se* $\mathrm{MCD}(a, n) = 1$.
(ii) $0_A \neq [\,a\,]_n \in A$ *è divisore dello zero se e solo se* $\mathrm{MCD}(a, n) \neq 1, n$.
(iii) *Se* $[\,a\,]_n \in A$ *è non unitario e non divisore dello zero allora* $[\,a\,]_n = 0_A$.

***D**imostrazione.* Per il lemma 2.7 a pagina 20 si può supporre $0 \leq a < n$.
(i) Come già osservato a pagina 23 un elemento $[\,a\,]_n$ è unitario se e solo se la congruenza lineare $ax \equiv 1 \ _{(n)}$ ammette soluzione.
Per il teorema 2.9 questo avviene se e solo se $\mathrm{MCD}(a, n) = 1$.
(ii) Supponiamo $d := \mathrm{MCD}(a, n) \neq 1, n$ ed $a \neq 0$. Ovviamente essendoci ricondotti al caso $0 < a < n$ non può essere $\mathrm{MCD}(a, n) = n$ e quindi la condizione diventa semplicemente $\mathrm{MCD}(a, n) \neq 1$. Allora $a = \widetilde{a}d$ e $n = \widetilde{n}d$ per qualche $\widetilde{a}$ e $\widetilde{n}$ con $\widetilde{n} \neq n$ perché $d \neq 1$. Ma allora, essendo $[\,\widetilde{n}\,]_n \neq [\,0\,]_n$ si ha che

$$[\,a\,]_n \cdot [\,\widetilde{n}\,]_n = [\,a\widetilde{n}\,]_n = [\,\widetilde{a}d\widetilde{n}\,]_n = [\,\widetilde{a}n\,]_n = [\,0\,]_n$$

e quindi $[\,a\,]_n$ è divisore dello zero. Viceversa [1] supponiamo che $d = 1$. Allora per il punto (i) $[\,a\,]_n$ è unitario e per il lemma 5.4 non è divisore dello zero.
(iii) Per esclusione. Se $[\,a\,]_n$ non è unitario allora per (i) $\mathrm{MCD}(a, n) \neq 1$. Se inoltre non è divisore dello zero allora per (ii) $\mathrm{MCD}(a, n) = 1, n$. Mettendo assieme le due cose si ottiene che $\mathrm{MCD}(a, n) = n$. Quindi $n \mid a$ e $[\,a\,]_n = [\,0\,]_n$. ∎

[1] Proviamo la contronominale della proposizione inversa.

5.1.2 Esempio: anelli di polinomi

Un esempio molto importante di anello è dato dagli anelli di polinomi. In questo paragrafo tratteremo la costruzione di un anello di polinomi partendo da un anello commutativo. La premessa comune a tutto il paragrafo è:

Sia $(A, \cdot)$ *un anello commutativo.*

Definizione 5.8 *Si dice polinomio sull'anello* A *una successione* $(a_0, a_1, \dots, a_i, \dots)$ *di elementi di* A *(intesa come funzione* $f : \mathbb{Z}_0 \to A$*) che sia definitivamente nulla. Cioè tale che:*

$$\exists\, n_0 \in \mathbb{Z}_0 : \ \forall\, n \geq n_0 \ \ \textit{si ha} \ \ a_n = \underline{0}_A$$

Gli elementi di A *che compaiono come termini della successione si dicono coefficienti del polinomio. Definiamo somma e prodotto di due polinomi (di elementi di* A*) come:*

$$(a_0, \dots, a_i, \dots) + (b_0, \dots, b_i, \dots) := (a_0 + b_0, \dots, a_i + b_i, \dots)$$

$$(a_0, \dots, a_i, \dots) \cdot (b_0, \dots, b_i, \dots) := (a_0 b_0, \dots, \sum_{h=0}^{i} a_k b_{i-h}, \dots)$$

È semplice verificare che rispetto a queste operazioni l'insieme dei polinomi su A è un *anello commutativo*. È possibile rappresentare i polinomi come espressioni formali introducendo un simbolo detto *indeterminata* e comunemente indicato con x.
Se $a_i = \underline{0}_A$ per ogni $i > n$ e $a_n \neq \underline{0}_A$ si pone:

$$a_n x^n + \ldots + a_1 x^1 + a_0 x^0 := (a_0, a_1, \dots, a_n, \underline{0}_A, \dots)$$

Per convenzione si scrive $a_1 x$ invece di $a_1 x^1$ e a_0 invece di $a_0 x^0$. Nella scrittura simbolica introdotta non vengono riportati i termini per cui $a_i = \underline{0}_A$. Con queste convenzioni le operazioni di somma e prodotto coincidono con quelle usuali.

Definizione 5.9 *L'anello dei polinomi su* A *verrá indicato con* $A[x]$*. Lo zero* $0_{A[x]}$ *e l'unità* $1_{A[x]}$ *dell'anello sono dati da:*

$$0_{A[x]} = (0_A, \dots) \qquad\qquad 1_{A[x]} = (1_A, 0_A, \dots)$$

Un polinomio della forma simbolica $a_i x^i$ *è detto monomio. Un generico polinomio* $a_n x^n + \ldots + a_1 x^1 + a_0 x^0$ *con* a_n *non nullo è detto monico se* $a_n = 1_A$*.*

Osservazioni Si osservi che sulla base della definizione data si ha che due polinomi sono uguali sse hanno gli stessi elementi nelle stesse posizioni (visti come successioni a valori in A). Si deve prestare attenzione alla differenza che intercorre tra il concetto di *funzione polinomiale* (comunemente usata in contesti analitici) e il concetto di polinomio. Ad ogni polinomio è associata una funzione polinomiale $F : A \to A$ definita attraverso la notazione simbolica:

$$a \longmapsto a_n a^n + \ldots + a_1 a + a_0 \in A$$

dove però la scrittura non è da considerarsi simbolo (ma un "conto" in A). Nel caso dei polinomi sull'anello $(\mathbb{R}, +, \cdot)$ vi è una corrispondenza biunivoca tra funzioni polinomiali e polinomi ma in generale questo non è vero. Si consideri a titolo di esempio l'anello

$$A = \mathbb{Z}/2\mathbb{Z} = \{\, [0]_n, [1]_n \}$$

e il polinomio $a(x) := x^2 - x$. Allora si vede subito (facendo i calcoli modulo 2) che $a(x)$ ha come funzione polinomiale associata la funzione nulla ma non è il polinomio nullo! [1] Si osservi inoltre che i monomi del tipo ax^0 formano un sottoanello dell'anello $A[x]$ isomorfo ad A. Previa l'identificazione di a con ax^0 possiamo considerare A come un sottoanello di $A[x]$.

Definizione 5.10 *Si definisce grado di un polinomio non nullo* $a(x) = a_n x^n + \ldots + a_0$ *con* $a_n \neq 0_A$ *il numero* n. *Il termine* a_m *viene detto coefficiente direttivo di* $a(x)$. *Il polinomio nullo ha convenzionalmente grado* -1. *Scriviamo quindi:*

$$\mathrm{gr}(a(x)) := n$$

I polinomi di grado 0 *si dicono costanti*[2].

Osservazione Se $a(x)$ e $b(x)$ sono due polinomi allora la somma $a(x) + b(x)$ non può ovviamente superare il grado massimo. Potrebbe però essere minore basti pensare ai polinomi sull'anello $\mathbb{R}[x]$ dati da:

$$a(x) := (3, 5, 0, \ldots) = 5x + 3 \quad \text{e} \quad b(x) := (1, -5, 0, \ldots) = -5x + 1$$

Che hanno entrambi grado 1 ma la loro somma ha grado 0. Per quanto riguarda il prodotto $a(x)b(x)$ di due generici polinomi si ha (pensando alla scrittura simbolica usuale) che il grado è al più pari alla somma dei gradi dei due polinomi. In $\mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$ si ha che è esattamente uguale alla somma dei gradi ma se ad esempio consideriamo l'anello $\mathbb{Z}/6\mathbb{Z}[x]$ si ha che i due polinomi:

$$a(x) := ([0]_6, [3]_6, [0]_6, \ldots) = [3]_6 x \quad \text{e} \quad b(x) := ([0]_6, [2]_6, [0]_6, \ldots) = [2]_6 x$$

hanno grado 1 ma il loro prodotto è il polinomio nullo che ha grado -1. Possiamo quindi riassumere quanto detto nel seguente lemma.

Lemma 5.6 *Se* $A[x]$ *è un anello di polonomi e* $a(x), b(x) \in A[x]$ *allora:*
(i) $\mathrm{gr}(a(x) + b(x)) \leq \max(\mathrm{gr}(a(x)), \mathrm{gr}(b(x)))$
(ii) $\mathrm{gr}(a(x)b(x)) \leq \mathrm{gr}(a(x)) + \mathrm{gr}(b(x))$
In (ii) *vale l'uguaglianza se* A *è privo di divisori dello zero.*

Riassumiamo le proprietà di un anello A che vengono ereditate nell'anello $A[x]$.

Lemma 5.7 *Se* A *è un anello allora:*
(i) A *privo di divisori dello zero* $\implies$ $A[x]$ *privo di divisori dello zero.*
(ii) A *commutativo* $\implies$ $A[x]$ *commutativo.*
In particolare se A *è un dominio allora* $A[x]$ *lo è.*

Lemma 5.8 *Se* A *è un dominio allora gli elementi unitari del dominio* $A[x]$ *sono tutti e soli gli elementi unitari di* $A \subseteq A[x]$ [3]. *In particolare se* $A = F$ *è un campo, i polinomi invertibili sono tutti e sole le costanti (non nulle!).*

[1] In generale in un qualsiasi campo finito avente ordine q il polinomio $x^q - x$ ha funzione associata nulla.

[2] Se identifichiamo $a \mapsto ax^0$ le *costanti* sono gli elementi non nulli di A (si parla di A come l'anello delle costanti).

[3] Con l'identificazione $a \mapsto ax^0$.

***D**imostrazione.* Siano $a(x) = a_n x^n + \ldots + a_0$ e $b(x) = b_m x^m + \ldots + b_0$ con $a_n, b_n \neq 0_A$. Allora $a(x)b(x) = a_n b_n x^{n+m} + \ldots + a_0 b_0$. Essendo A un dominio $a_n b_n \neq 0$ e quindi $\mathrm{gr}(a(x)b(x)) = n+m$. In particolare $a(x)b(x) = 1_A$ se e e solo se $a(x) = a_0,\ b(x) = b_0$ e si ha $a_0 b_0 = 1_A$. Quindi gli elementi unitari di $A[x]$ sono gli elementi della forma $a(x) = a_0$ con a_0 invertibile ($b_0 = a_0^{-1}$). ■

Osservazione Se A non è un dominio questo fatto non vale. Ad esempio nell'anello $A = \mathbb{Z}/4\mathbb{Z}$ si ha (intendendo con ogni coefficiente a_i la classe $[\, a_i \,]_4$):

$$(2x+1)(2x+1) = 4x^2 + 4x + 1 = 1 \qquad (4 \equiv 0 \ {}_{(4)})$$

5.1.3 Teorema di Eulero-Fermat

Definizione 5.11 *Si dice funzione di Eulero la funzione che ad ogni intero $n > 1$ associa il numero $\phi(n)$ degli interi positivi minori di n, coprimi con n.*

ESEMPIO Ad esempio $\phi(2) = 1$, $\phi(2) = 2$, $\phi(4) = 2$, $\phi(6) = 2$. In generale se p è primo (e quindi coprimo con ogni $0 < n < p$) si ha che $\phi(p) = p - 1$.

Teorema 5.9 (Eulero-Fermat)
Per ogni $n > 1$ e per ogni $a \in \mathbb{Z}$ tale che $\mathrm{MCD}(a, n) = 1$ *si ha*

$$a^{\phi(n)} \equiv 1 \ _{(n)}$$

***D**imostrazione.* Consideriamo l'anello $A := (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$.
Per la proposizione 5.5 un elemento $[\,a\,]_n \in A$ è unitario se e solo se $\mathrm{MCD}(a, n) = 1$. L'insieme $\mathcal{U}$ degli elementi unitari di A forma un gruppo moltiplicativo il cui ordine è il numero degli elementi unitari che quindi coincide con il numero $\phi(n)$ degli interi minori di n coprimi con n. In particolare (per 3.10) si ha $[\,a\,]_n^{\phi(n)} = [\,1\,]_n$. ■

Corollario 5.10 (Piccolo teorema di Fermat)
Se p è un numero primo ed $a \in \mathbb{Z}$ tale che $p \nmid a$ allora $a^{p-1} \equiv 0 \ _{(p)}$

***D**imostrazione.* Se p è un primo e $p \nmid a$ allora p ed a sono coprimi. Inoltre se p è primo $\phi(p) = p - 1$. La tesi segue dal teorema precedente. ■

Proposizione 5.11 *Valgono le seguenti affermazioni:*
(i) *Se p è un numero primo ed $m > 0$ allora $\phi(p^m) = p^m - p^{m-1}$.*
(ii) *Se* $\mathrm{MCD}(a, b) = 1$ *allora $\phi(ab) = \phi(a) \cdot \phi(b)$.*

OSSERVAZIONI

1. Come conseguenza del teorema di Eulero-Fermat $[\,a\,]_n \in \mathbb{Z}/n\mathbb{Z}$ è un elemento unitario, allora $[\,a\,]_n^{\phi(n)-1} \cdot [\,a\,]_n = [\,a\,]_n^{\phi(n)} = [\,1\,]_n \implies [\,a\,]_n^{-1} = [\,a\,]_n^{\phi(n)-1}$.
   In particolare se p è primo $[\,a\,]_p^{-1} = [\,a\,]_p^{p-2}$.
2. Supponiamo di voler calcolare $\phi(n)$ per un certo $n > 0$. Per il teorema fondamentale dell'aritmetica $n = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$ per dei primi p_i. Quindi per la proposizione precedente

   $$\phi(n) = \phi(p_1^{m_1}) \ldots \phi(p_k^{m_k}) = (p^{m_1} - p^{m_1-1}) \ldots (p^{m_k} - p^{m_k-1})$$

   Segue che se $n \neq 2$ allora $\phi(n)$ è pari perché prodotto di numeri pari[1].

[1] $p^m - p^{m-1} = p^{m-1}(p-1)$ è pari se e solo se uno dei due fattori è pari. Se p è dispari $p - 1$ è pari e quindi $p^m - p^{m-1}$ è pari. L'unico numero primo pari è 2 e in tal caso $\phi(2) = 1$ è dispari.

5.2 Corpi, campi

Definizione 5.12 *Un anello K si dice corpo se è non banale ($|K| > 1$) e se ogni elemento non nullo di K è invertibile rispetto al prodotto. Cioè se $\mathcal{U} = K^* = K \setminus \{0_K\}$ (i.e. ogni elemento non nullo è unitario). In altre parole se K^* è un gruppo moltiplicativo. Se K è commutativo diremo che è un campo.*

Osservazione Un corpo K è privo di divisori dello zero in quanto un elemento unitario in un anello non è divisore dello zero. Come già osservato il viceversa non è vero in generale (basta pensare a $\mathbb{Z}$). Se però K è finito le cose cambiano:

Teorema 5.12 *Un anello non banale A finito e privo di divisori dello zero è un corpo. In particolare un dominio finito è un campo.*

***D**imostrazione.* Essendo A non banale esiste $a \in A,\ a \neq 0$. Essendo A finito esistono due interi $r > s$ tali che $a^r = a^s$. Si ha che $a^s \neq 0$ in quanto A è privo di divisori dello zero. Valgono inoltre le leggi di cancellazione. Quindi:

$$a^r - a^s = 0_A \implies a^s(a^{r-s} - 1_A) = 0_A \implies a^{r-s} = 1_A$$

Poniamo allora $h := r - s$. Se $h = 1,\ a = 1_A$. Se $h > 1\ \ a^h = a \cdot a^{h-1} = a^{h-1} \cdot a = 1_A$. Segue che a^{h-1} è l'inverso di a e quindi che a è unitario. ∎

In realtà vale il seguente teorema.

Teorema 5.13 (di Weddenburn) *Ogni corpo finito è un campo.*

Definizione 5.13 *Sia E un corpo (risp. campo). Un sottoinsieme $K \subseteq E$ si dice sottocorpo (risp. sottocampo) di E se $1 < |K|$, K è un sottoanello ed è chiuso rispetto all'inverso e al prodotto. Cioè se $K^* \leq E^*$.*

Proposizione 5.14 (Criterio per sottocorpi (sottocampi)) *Un sottoinsieme K ($|K| > 1$) di un corpo (risp. campo) è un sottocorpo (risp. sottocampo) se:*
(i) $\forall\, a, b \in K:\quad a - b \in K$.
(ii) $\forall\, a \in K,\ \ \forall\, b \in K,\ b \neq 0_K\ \ si\ ha\ \ ab^{-1} \in K$.

***D**imostrazione.* Una immediata conseguenza del criterio 3.5 applicato due volte. ∎

Corollario 5.15 *L'anello $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ è un campo se e solo se n è primo.*

***D**imostrazione.* Per il teorema 5.12 sappiamo che un anello finito privo di divisori dello zero è un corpo (se l'anello è commutativo è un campo). D'altra parte, per quanto osservato a pagina 62, $\mathbb{Z}/n\mathbb{Z}$ è privo di divisori dello zero se e solo se n è primo. ∎

5.3 Congruenze in un anello, ideali

Definizione 5.14 *Una relazione di equivalenza definita in un anello A si dice congruenza quando è compatibile con la somma e con il prodotto definiti in A. Cioè quando:*

$$a \sim a',\ \ b \sim b' \implies (a+b) \sim (a'+b')$$
$$a \sim a',\ \ b \sim b' \implies (ab) \sim (a'b')$$

Il nucleo della congruenza di anelli è $N = [\,0_A\,]_\sim$.

Definizione 5.15
Un sottoinsieme I di un anello A si dice ideale sinistro (risp. destro) dell'anello A se:
(i) *I è un sottogruppo del gruppo additivo $(A,+)$.*
(ii) *I è se è chiuso rispetto al prodotto a sinistra (risp. destra) per un qualsiasi elemento dell'anello. Cioè:*

$$\forall\, i \in I,\ \forall\, x \in A \quad \textit{si ha} \quad xi \in I \qquad \textit{(risp. } ix \in I\textit{)}$$

Un ideale sia sinistro che destro si dice bilatero (o, semplicemente, ideale).

Osservazioni

1. Se un ideale I contiene l'unità allora $\forall\, x \in A,\ x \cdot 1_A \in I$ e quindi $I = A$. Un ideale contiene necessariamente lo zero dell'anello.
2. Ogni anello contiene gli *ideali banali* che sono $\{\,0_A\}$ e A.
3. Un ideale bilatero è chiuso rispetto al prodotto definito in A. Ovviamente se l'anello è commutativo tutti gli ideali sono bilateri.

Esempio Nell'anello $(\mathrm{Mat}(3,\mathbb{A}),+,\cdot)$ l'insieme:

$$I_s = \left\{ \left(\begin{array}{c|cc} a_1 & 0 & 0 \\ a_2 & 0 & 0 \\ a_3 & 0 & 0 \end{array} \right) :\ \ a_1,a_2,a_3 \in A \right\}$$

È un ideale sinistro (ma non destro). In modo analogo l'insieme:

$$I_d = \left\{ \left(\begin{array}{ccc} a_1 & a_2 & a_3 \\ \hline 0 & 0 & 0 \\ 0 & 0 & 0 \end{array} \right) :\ \ a_1,a_2,a_3 \in A \right\}$$

È un ideale destro ma non sinistro.

Lemma 5.16 *Siano A, B anelli. Sia $f : A \to B$ un morfismo. Allora:*
(i) *Se $J \subseteq B$ è un ideale sinistro (destro, bilatero) allora anche $f^{-1}(J)$ è un ideale sinistro (destro, bilatero) di A.*
(ii) *Se $I \subseteq A$ è un ideale sinistro (destro, bilatero) ed f è suriettiva allora $f(A)$ è un ideale sinistro (destro, bilatero) di B.*

***D**imostrazione.* Essendo f un morfismo di anelli in particolare è un morfismo nei gruppi $(A,+)$ e $(B,+)$. Quindi per il lemma 4.17 gli insiemi considerati sono dei sottogruppi additivi. Resta da provare che sono chiusi rispetto al prodotto (a sinistra ad esempio). (i) Se $a \in A$ e $a_0 \in f^{-1}(J)$ allora $f(aa_0) = f(a)f(a_0)$. Il primo fattore sta in B e il secondo in J. Quindi $aa_0 \in f^{-1}(J)$. (ii) Se $b \in B$ e $b_0 \in f(I)$ allora $b_0 = f(i)$ per qualche $i \in I$. Per la suriettività di f si ha $b = f(a)$ per qualche $a \in A$. Segue che $bb_0 = f(a)f(i) = f(ai) \in f(I)$ in quanto $ai \in I$ (I è un ideale). ∎

Proposizione 5.17 *Il nucleo di una congruenza in un anello è un ideale (bilatero). Inversamente sia I un ideale (bilatero) di A e sia D_I la relazione su A definita ponendo:*

$$aD_Ib \iff \exists\, i \in I \quad \textit{tale che} \quad b = i + a$$

Allora D_I è una congruenza avente nucleo I.

***D**imostrazione.* La prima parte è conseguenza immediata della definizione. Inversamente, I è per definizione un sottogruppo del gruppo additivo $(A, +)$. Essendo tale gruppo abeliano si ha che I è un sottogruppo normale. Per la proposizione 4.8 pagina 39 la relazione D_I (che coincide con la D_H definita a pagina 37) é una congruenza avente nucleo I. Proviamo che è compatibile con il prodotto. Supponiamo che aD_Ia' e bD_Ib'. Allora $a' = i_1 + a$ e $b' = i_2 + b$ per qualche $i_1, i_2 \in I$. Si ha quindi $a'b' = (i_1i_2 + i_1b + ai_2) + ab = i + ab$ in quanto I è bilatero e quindi tutti e tre gli addendi stanno in I (e la somma anche, essendo $I \leq (A, +)$). ■

5.4 Anelli quoziente e teoremi di isomorfismo

Enunciati del tutto analoghi a quelli per i gruppi valgono per gli anelli.

Teorema 5.18 (Anello quoziente ed epimorfismo canonico)
Sia $(A,+,\cdot)$ un anello e I un ideale di A. Allora l'insieme quoziente di A rispetto alla congruenza D_I (i cui oggetti sono i laterali $I+a$) é un anello rispetto alle operazioni indotte:

$$\textit{Somma:}\quad (I+a)+(I+b)=I+(a+b)$$
$$\textit{Prodotto:}\quad (I+a)\cdot(I+b)=I+(ab)$$

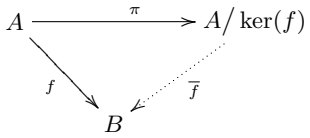
Questo anello si denota con $(A/I,+,\cdot)$ e si parla di anello quoziente di A rispetto all'ideale I. La projezione canonica $\pi: A\to A/I$ è un epimorfismo detto epimorfismo canonico.

***D**imostrazione.* Rispetto alla somma c'è una struttura di gruppo quoziente, per il teorema 4.19. La commutatività della somma è ereditata così come l'associatività del prodotto. L'unità dell'anello è per come sono definite le operazioni la classe $[\,1_A\,]_{D_I} = I+1_A$. Le proprietà distributive sono verificate. Ad esempio: $(I+a)((I+b)+(I+c)) = (I+a)(I+(b+c)) = I+(a(b+c)) = I+(ab+ac) = (I+a)(I+b)+(I+a)(I+c)$. Il resto dell'enunciato è ovvio. ∎

Teorema 5.19 (Teorema d'omomorfismo per gli anelli)
Siano A e B anelli e $f: A\to B$ un omomorfismo. Allora:
(i) *La relazione di equivalenza R associata ad f è una congruenza in A.*
(ii) *Esiste uno ed un solo omomorfismo $\overline{f}: A/\ker(f)\to B$ tale che:*

$$f=\overline{f}\circ\pi \qquad \textit{(Proprietà universale dell'epimorfismo canonico)}$$

Cioè tale da rendere commutativo il seguente diagramma:



$\overline{f}$ è sempre un monomorfismo ed è un isomorfismo se e solo se f è un epimorfismo.

***D**imostrazione.* Gran parte dell'enunciato è il ben noto teorema d'omomorfismo per i gruppi. Resta da provare che: (i) Se $f(a)=f(a')$ e $f(b)=f(b')$ allora $f(ab)=f(a)f(b)=f(a')f(b')=f(a'b')$. (ii) $\overline{f}$ definita da $\ker(f)+a\longmapsto f(a)$ è ben definita. Conserva il prodotto: $\overline{f}((\ker(f)+a)(\ker(f)+b))=\overline{f}(\ker(f)+(ab))=f(ab)=f(a)f(b)=\overline{f}((\ker(f)+a))\overline{f}((\ker(f)+b))$. Infine $\overline{f}(\ker(f)+1_A)=f(1_A)=1_B$. ∎

Quindi se B è un anello immagine epimorfa di A allora può essere identificato con un opportuno anello quoziente di A.

Lemma 5.20 *Siano I,J ideali di un anello A. Allora:*
(i) *$I\cap J$ è un ideale.*
(ii) *$I+J:=\{\,i+j:\ i\in I,\ j\in J\,\}$ è un ideale.*
(iii) *$IJ:=\{\,$somme finite $\sum a_rb_s:\ a_r\in I,\ b_s\in I\,\}$ è un ideale.*

ESEMPIO Quali sono le immagini epimorfe di $\mathbb{Z}$? Per quanto visto equivale a cercare gli ideali e gli anelli quoziente. *Gli ideali di $\mathbb{Z}$ sono tutti e soli i sottogruppi di $(\mathbb{Z}, +)$.* Infatti un sottogruppo H di $(\mathbb{Z}, +)$ è un ideale se $\forall\, z \in \mathbb{Z},\ \forall\, h \in H$ si ha $zh \in H$. D'altra parte zh è il multiplo additivo di h secondo z. Quindi ogni sottogruppo del gruppo additivo è un ideale (e viceversa). Quindi le immagini epimorfe di $\mathbb{Z}$ a meno di isomorfismi sono gli anelli quozienti $\mathbb{Z}/n\mathbb{Z}$. Se $n = 0$; $\mathbb{Z}/n\mathbb{Z} \backsimeq \mathbb{Z}$. Se $n = 1$; $\mathbb{Z}/n\mathbb{Z} = \{\, 0_A\}$. se $|n| > 1$; $\mathbb{Z}/n\mathbb{Z}$ è l'anello delle classi resto modulo n.

Vediamo ora i teoremi di isomorfismo per gli anelli.

Teorema 5.21 (Primo teorema d'isomorfismo)
Sia A un anello e I un ideale. Sia J un sottoanello di A. Allora $I + J$ è un sottoanello di A, $I \cap J$ é un ideale di J e si ha:

$$\frac{I+J}{I} \backsimeq \frac{J}{I \cap J}$$

***D**imostrazione.* Se si considera l'applicazione $J \to (I + J)/I$ definita da

$$\forall\, j \in J \qquad j \longmapsto I + j$$

tale applicazione è un epimorfismo avente nucleo $I \cap J$.
La tesi segue dunque dal teorema d'omomorfismo. ∎

Teorema 5.22 (secondo teorema d'isomorfismo)
Sia A un anello e siano I, J ideali di A tali che $I \subseteq J$. Allora J/I è un ideale di A/I e si ha

$$\frac{A/I}{J/I} \backsimeq \frac{A}{J}$$

***D**imostrazione.* **Da completare.** ∎

5.5 Caratteristica di un anello

Un esempio notevole è quello che conduce alla nozione di *caratteristica di un anello.* Sia A un anello. Consideriamo l'applicazione $C : \mathbb{Z} \to A$ definita ponendo:

$$\forall\, z \in \mathbb{Z} \qquad z \overset{C}{\longmapsto} z1_A \qquad \textit{(multiplo additivo secondo } z\textit{)}$$

C è un morfismo di anelli. Infatti:
(i) Per la proprietà delle potenze [1] : $(z_1 + z_2)1_A = z_1 1_A + z_2 1_A$.
(ii) $(z_1 z_2)1_A = z_1(z_2 1_A) = z_1(1_A \cdot z_2 1_A) = (z_1 1_A) \cdot (z_2 1_A)$
(iii) $11_A = 1_A$.
Si ha:

$$\ker C = \{\, z \in \mathbb{Z} :\ z1_A = 0_A \,\}$$

Ci sono due possibilità. Se $o(1_A) = \infty$ allora per la proposizione 3.10 pagina 31 la funzione potenza (multiplo) è iniettiva e quindi, per il lemma 4.21 si ha che $\ker C = \{0\}$. In questo caso diremo che l'anello A ha *caratteristica* 0. Se $o(1_A) = n < \infty$ allora $\ker C = \{$ multipli di $n \,\} = n\mathbb{Z}$. Diremo in questo caso che l'anello ha *caratteristica* n.

Definizione 5.16 *Sia l'omomorfismo C come nell'esempio precedente. Si dice che un anello A ha caratteristica* 0 *(e si scrive* $\mathrm{Car}(A) = 0$*) se $o(1_A) = \infty$ nel gruppo $(A, +)$. Si dice che A ha caratteristica n (e si scrive* $\mathrm{Car}(A) = n$*) se $o(1_A) = n$.*

$$\textit{Se } \mathrm{Car}(A) = 0 \quad \textit{allora} \quad C(\mathbb{Z}) \backsimeq \mathbb{Z}$$
$$\textit{Se } \mathrm{Car}(A) = n \quad \textit{allora} \quad C(\mathbb{Z}) \backsimeq \mathbb{Z}/n\mathbb{Z}$$

Corollario 5.23 *Sia D un dominio di integrità di caratteristica non zero. Allora* $\mathrm{Car}(D) = p$ *è un numero primo.*

***D**imostrazione.* Se la caratteristica non è zero allora $\mathbb{Z}/n\mathbb{Z} \backsimeq C(\mathbb{Z}) \leq D$ è un sottoanello (e quindi un dominio) di D isomorfo a $\mathbb{Z}/n\mathbb{Z}$. Ma $\mathbb{Z}/n\mathbb{Z}$ è privo di divisori dello zero se e solo se n è primo. ∎

Osservazione Ovviamente un anello finito non può avere caratteristica nulla.

[1] In forma additiva, in questo caso ("seduta in orizzontale" :-)).

5.6 Ideali principali, domini a ideali principali

Lemma 5.24 *Sia R un anello. Si ponga:*

$$(a)_s := Ra = \{\, xa : \ \forall\, x \in R \,\} \qquad (a)_d := aR = \{\, ax : \ \forall\, x \in R \,\}$$

(i) $(a)_s$ *(risp.* $(a)_d$*) è un ideale sinistro (destro) di* R.
(ii) *Se* I_s *è un ideale sinistro di* R *e* $a \in I_s$*, allora* $(a)_s \subseteq I_s$ *(analogamente a destra).*
(iii) *Sia* R *commutativo. Allora* $(a)_s = (a)_d =: (a)_s = Ra$*. Si ha che:*

$$(a) = R \iff a \text{ è un elemento unitario di } R \ \ (\textit{i.e. } a \in \mathcal{U})$$

***D**imostrazione.* (i) $(a)_s$ è un sottogruppo di $(A, +)$ in quanto per ogni $x_1, x_2 \in R$ si ha $x_1a - x_2a = (x_1 - x_2)a \in (a)_s$. $(s)_s$ è chiuso rispetto al prodotto a sinistra in quanto per ogni $xa \in (a)_s$ e per ogni $y \in R$ si ha $y(xa) = (yx)a \in (a)_s$.
Segue che è un ideale. (ii) Se $a \in I_s$ allora $xa \in I_s$ e quindi $(a)_s \subseteq I_s$.
(iii) Supponiamo $R = Ra$. Allora $1_A \in Ra$ e quindi esiste $\widetilde{x} \in R$ tale che $1_A = \widetilde{x}a$. Ma allora $\widetilde{x}$ è l'inverso di a. Viceversa supponiamo $a \in \mathcal{U}$. Allora ogni y in R può essere scritto come $y \cdot 1_A = y \cdot (a^{-1}a) = (ya^{-1})a$. Posto $x := ya^{-1} \in R$ si ha che $y = xa \in Ra$. Segue che $R = Ra$. ∎

Osservazione Dunque *un ideale che non sia l'intero anello deve essere costituito da elementi non invertibili rispetto al prodotto.* Infatti l'argomento mostra che non appena $a \in I_s$ è invertibile allora ogni $y \in R$ si può scrivere come $(ya^{-1})a$ e quindi $y \in (a)_s \supseteq R$. Essendo $(a)_s \subseteq I_s \subseteq R$ si ha che $I_s = R$. In particolare *in un campo non ci sono ideali non banali.* Si osservi inoltre che l'ideale $I = \{\, 0 \,\}$ coincide con (0).

Definizione 5.17 *Sia R un anello commutativo. L'ideale $(a) = Ra$ prende il nome di ideale principale generato dall'elemento a.*

Definizione 5.18 (PID**)** *Un dominio D in cui ogni ideale è principale viene detto dominio a ideali principali (o dominio principale). Si usa abbreviare dicendo che D è un* PID *(principal ideal domain).*

Esempi

1. $(\mathbb{Z}, +, \cdot)$ è un dominio principale dove $(n) = n\mathbb{Z}$.
2. Se K è un campo il dominio dei polinomi $K[x]$ su K è un dominio principale (attenzione! questo non è più vero se K non è un campo).
3. D dominio euclideo $\implies$ D dominio a ideali principali.

Definizione 5.19 *Sia A un anello commutativo. Siano $a_1, \ldots, a_s \in R$.*
Denotiamo con

$$(a_1, \ldots, a_s) := Ra_1 + \ldots + Ra_s \qquad \textit{(Ideale somma)}$$

l'insieme di tutte le combinazioni lineari a coefficienti in R (somme con un numero finito di elementi della forma x_ia_j). Diremo che $(a_1, \ldots, a_s)$ è l'ideale generato da $a_1, \ldots, a_s$.

Osservazioni

1. Secondo questa definizione la scrittura definita nel lemma 5.24 coincide con la nozione di ideale generato da un elemento a.

2. Dato un anello K, l'anello $K[x]$ è a ideali principali se e solo se K è un campo.
3. Nell'anello $\mathbb{Z}[x]$ l'ideale $I = (2, x) = (2) + (x)$ non è principale. Infatti (2) è costituito dalle costanti pari e (x) da tutti i polinomi della forma kx con $k \in \mathbb{Z}$. Allora I è l'ideale dei polinomi con termine noto pari. Tuttavia non esiste un polinomio $\delta(x)$ che da solo generi l'ideale I. Infatti dovrebbe dividere i polinomi 2 e x e quindi dovrebbe essere il polinomio costante ± 1, il che è assurdo.

Proposizione 5.25 *Sia R un anello* commutativo [2] *($R \neq \{0_R\}$).*
R è un campo se e solo se gli unici ideali sono quelli banali.

***D**imostrazione.* In un campo un ideale che non contenga solo lo zero deve contenere almeno un elemento. Tale elemento è unitario e quindi l'ideale è tutto il campo. Se viceversa R non ha ideali non banali allora se $0_R \neq a \in R$ deve essere $Ra = R$. Segue che $1_R \in Ra$, ovvero esiste $r \in R$ tale che $ra = 1_R$. Dunque a è invertibile. ∎

È naturale a questo punto chiedersi quando avvenga che in un anello A commutativo $(a) = (b)$. La risposta nel caso in cui $A = D$ è un dominio di integrità è che *occorre e basta che a e b differiscano per un elemento unitario*:

Proposizione 5.26 *Sia D un dominio di integrità. Siano $a, b \in D$. Si ha:*

$$(a) = (b) \iff a = ub \qquad \text{per qualche } u \in \mathcal{U}.$$

***D**imostrazione.* Se $a = ub$ chiaramente $a \in (b)$ e quindi $(a) \subseteq (b)$. D'altra parte essendo u unitario si ha $u^{-1}a = b$ e quindi $(b) \subseteq (a)$. Inversamente se $(a) = (b)$ allora esistono $x_1, x_2 \in D$ tali che $a = x_1 b$ e $b = x_2 a$. Segue che $a = x_1 x_2 a$. Essendo D un dominio per (5.2) valgono le leggi di cancellazione e quindi $x_1 x_2 = 1_D$.
In particolare x_1 è unitario. ∎

Definizione 5.20 *Sia D un dominio di integrità. Diremo che $b \in D$ divide (o è un fattore) di $a \in D$ e scriveremo $b \mid a$ se esiste $c \in D$ tale che $a = bc$.*

Osservazioni

1. Ogni elemento di un dominio D è divisibile per ogni elemento unitario. Infatti se $u \in \mathcal{U}$ allora $a = u(u^{-1}a)$. Quindi dalla definizione, ponendo $b := u$ e $c := u^{-1}a$ si ha che $u \mid a$.
2. Ogni elemento che differisce da a per un unitario è un fattore di a. Gli elementi unitari e gli elementi che differiscono da a per un fattore unitario *fattori banali di a*. Ad esempio in $\mathbb{Z}$ i fattori banali di 24 sono $1, -1, 24, -24$. Un fattore non banale viene detto *fattore proprio*. .
3. La relazione $\sim$ che associa a e b se differiscono per $u \in \mathcal{U}$ è una relazione di equivalenza. Se $a \sim b$ dirà che a e b sono *associati*. Ovviamente per quanto osservato gli elementi unitari formano una unica classe di equivalenza rispetto a tale relazione (un elemento che differisce da un unitario per un unitario è a sua volta unitario). Infatti se $u_1, u_2 \in \mathcal{U}$ allora essendo $(\mathcal{U}, \cdot)$ un gruppo si ha che $u_2 u_1^{-1} \in \mathcal{U}$. Allora posto $u_3 := u_2 u_1^{-1}$ si ha che $u_3 u_1 = u_2$.
4. $(a) \subseteq (b)$ *se e solo se* $b \mid a$. Infatti $(a) \subseteq (b) \Rightarrow a \in (b) \Rightarrow a = yb$ per qualche $y \in D$. Segue che $b \mid a$. Inversamente se $b \mid a$ allora $bc = a$ per qualche $c \in D$. Allora $a \in (b)$ e quindi $(a) \subseteq (b)$. Quindi $(a) = (b)$ *se e solo se* $b \mid a$ *e* $a \mid b$.

[2] Attenzione! questo enunciato è falso se R non è commutativo!

5. $(a) \subset (b)$ *se e solo se* b *è un fattore proprio di* a. Infatti $(a) \subset (b) \iff a = yb$ ma $\nexists\, x \in D$ tale che $b = xa$. Essendo $a = yb = yxa \iff xy = 1_A$ si ha che y non è unitario. Quindi essendo $(a) \neq D$ e $(b) \neq D$ si ha che anche a e b non sono unitari e quindi che $a = yb$ è una fattorizzazione non banale di a. In particolare se un elemento x è irriducibile allora non esiste un ideale (y) tale che $(x) \subset (y) \subset D$ (perché y dovrebbe essere fattore proprio di x). Per il viceversa basta ripercorrere il ragionamento all'indietro.

Definizione 5.21 *Sia* D *un dominio e sia* $0_D \neq p \notin \mathcal{U}$ *un elemento* non unitario.
(i) p *si dice primo se* $\forall\, a, b \in D \quad p \mid ab \implies p \mid a \ \vee \ p \mid b$.
(ii) p *si dice irriducibile se ammette solo fattori banali (cioè se* $p = u(u^{-1}p)$ *è l'unico modo di fattorizzare* p *in* D*). Equivalentemente un elemento* p *è irriducibile se è non unitario e non può essere scritto come prodotto di due elementi non unitari.*

Osservazione Se a è irriducibile in D e $\widetilde{a} \sim a$ è un associato di a allora anche $\widetilde{a}$ è irriducibile. Infatti $\widetilde{a} = ua$ ammette solo fattori irriducibili perché a è irriducibile e il prodotto di due elementi unitari è unitario.

Proposizione 5.27 *In un dominio di integrità ogni elemento primo è irriducibile.*

D*imostrazione.* Sia p un primo in un dominio. Allora se $p = ab$ si ha, essendo p primo, che $p \mid a$ o $p \mid b$. A meno di scambiare a e b possiamo supporre che $p \mid a$. Allora $pq = a$ per qualche elemento q. È evidente che non può essere $q = 0_D$ perché altrimenti $p = 0_D$ non sarebbe primo. Ma allora si ottiene

$$p = ab = pqb \implies p(1_D - qb) = 0_D$$

ed essendo D un dominio e $p \neq 0_D$ deve essere necessariamente $qb = 1_D$. Segue che b è unitario. Quindi p non si può scrivere come prodotto di due elementi non unitari. ∎

5.7 Ideali primi e ideali massimali in un anello

Definizione 5.22 *Sia R un anello e sia $I \neq R$ un ideale di R. Siano $a, b \in R$.*
(i) *L'ideale I si dice primo se $xy \in I \implies x \in I \ \vee \ y \in I$.*
(ii) *I si dice massimale se per ogni ideale J tale che $I \subseteq J \subseteq R$ si ha necessariamente $J = I$ oppure $J = R$.*

Osservazioni

1. Un ideale I è massimale se e solo se non esiste alcun ideale J tale che $I \subset J \subset A$.
2. Se $R = D$ è un dominio allora (a) é un ideale primo se e solo se a è primo. Infatti $xy \in (a) = Ra \Leftrightarrow a \mid xy\,,\ x \in (a) \Leftrightarrow a \mid x$ e $y \in (a) \Leftrightarrow a \mid y\,.$
3. $\{\,0_R\}$ è primo se e solo se R non ha divisori dello zero.
4. In un dominio a ideali principali ogni ideale primo è massimale.

Proposizione 5.28 *Sia A un anello e I un ideale di A.*
L'epimorfismo canonico $\pi : A \to A/I$ induce una bijezione fra gli ideali di A che contengono I e tutti gli ideali dell'anello quoziente A/I.

***D**imostrazione.* Per ogni ideale J di A, $\pi(J)$ è un ideale di A/I (per 5.16). Dunque π induce una mappa $J \mapsto \pi(J)$. Mostriamo che è bigettiva. Se $\pi(J_1) = \pi(J_2)$ allora $\forall\, j_1 \in J_1 \ \ \exists j_2 \in J_2$ tale che $I + j_1 = I + j_2$. Ma questo implica che $j_1 = i + j_2$ e quindi $j_1 \subseteq J_2$. D'altra parte, per simmetria, si ha $J_2 \subseteq J_1$ e quindi $J_1 = J_2$. Quindi l'applicazione è iniettiva. Proviamo la suriettività. Se $\overline{J}$ è un ideale di A/I allora la sua preimmagine $J = \pi^{-1}(\overline{J})$ è un'ideale contenente I in quanto I è lo zero di A/I e quindi sta in $\overline{J}$. Per costruzione si ha $\pi(J) = \overline{J}$. ∎

Teorema 5.29 *Sia A un anello* commutativo *e $I \neq A$ un ideale di A.*
(i) *I è primo $\iff$ A/I è un dominio.*
(ii) *I è massimale $\iff$ A/I è un campo.*
In particolare ogni ideale massimale è primo.

***D**imostrazione.* (i) Si ha che $ab \in I \ \Leftrightarrow \ I + ab = I,\ a \in I \ \Leftrightarrow \ I + a = I$ e $b \in I \ \Leftrightarrow \ I + b = I$. Quindi la condizione $ab \in I \implies a \in I \ \vee \ b \in I$ equivale alla legge di annullamento del prodotto:

$$(I + a)(I + b) = I + ab \iff I + a = I \ \text{ oppure } \ I + b = I$$

Condizione a sua volta equivalente ad essere un dominio.
(ii) Se I è massimale in A allora gli ideali che contengono I sono solo I ed A (in particolare sono due). Essendoci una bijezione tra gli ideali di A che contengono I e gli ideali di A/I si ha che A/I ha solo gli ideali banali e non è un anello banale (in quanto $I \neq A$). Per 5.25 è quindi un campo. ∎

5.8 Domini euclidei

Definizione 5.23 (ED) *Un dominio D ($D \neq \{0_D\}$) si dice euclideo e si scrive* ED *(euclidean domain) se esiste un'applicazione $\nu : D^* = D \setminus \{0_D\} \to \mathbb{Z}_0$ tale che:*
(i) $\forall\, a, b \in D \quad \nu(a) \leq \nu(ab)$.
(ii) $\forall\, a \in D,\ \forall\, b \in D^* \quad \exists\, q, r \in D$ *tali che* $a = bq + r$ *e sia* $r = 0_D$ *oppure* $\nu(r) < \nu(b)$.
La funzione ν si chiama grado o norma definita su D^*.
Gli elementi q ed r si dicono quoziente e resto.

Osservazione Non si richiede l'unicità di quoziente e resto e non si richiede che la funzione ν sia definita in 0_D. In alcuni casi particolari si definisce la norma anche nello zero ma in generale no.

Esempi

1. Nell'insieme $\mathbb{Z}$ dei numeri interi definendo la norma come il valore assoluto ($\nu(a) = |a|$) si ottiene un dominio euclideo dove le priprietà (i) e (ii) sono banalmente verificate dalla divisione tra numeri interi.
2. L'insieme $\mathbb{C}$ dei numeri complessi con la norma data dal modulo di un numero complesso $\nu(x + iy) = x^2 + y^2$ è un dominio euclideo.
3. L'insieme $F[x]$ dei polinomi a coefficienti un un campo F è un dominio euclideo rispetto alla norma data dal grado di un polinomio:$\nu(a(x)) = \mathrm{gr}(a(x))$.
4. L'insieme $\mathbb{Z}[i]$ dei numeri complessi della forma $n + im$ con $m, n \in \mathbb{Z}$ è un dominio euclideo rispetto alla norma data dal modulo di un numero complesso.

Quello che si verifica è che l'insieme dei domini euclidei è un sottoinsieme dei domini a ideali principali (vedi definizione 5.18). Infatti ogni dominio euclideo è a ideali principali, come mostra il seguente:

Teorema 5.30 *Ogni* ED *è* PID.

***D**imostrazione.* Sia D un ED. Sia $(0_D) \neq I$ un ideale di D. Ogni elemento a non nullo di I ha grado $\nu(a)$. Per il principio del buon ordinamento esiste un $b \in I$ tale che $\nu(b)$ è il minimo fra tutti gli elementi non nulli di D.

Per ogni $a \in I$, $\exists\, q, r \in D$ tali che $a = bq + r$ e sia $r = 0_D$ oppure $\nu(r) < \nu(b)$. Segue che $r = a - bq \in I$ in quanto $bq \in I$. Per la scelta minimale di b in I deve essere $r = 0_D$. Segue che $a = bq \in (b) \implies I \subseteq (b)$. D'altra parte $b \in I \implies (b) \subseteq I$. Quindi l'ideale I è generato da b. ∎

Definizione 5.24 *Sia D un dominio e siano $a, b \in D^*$. Si dice che $d \in D$ è un massimo comun divisore tra a e b e si scrive $d = \mathrm{MCD}(a, b)$ se:*
(i) *d divide sia a che b.*
(ii) *Per ogni $c \in D \quad c \mid a \ \ e \ \ c \mid b \implies c \mid d$.*

Per dualità si ottiene la definizione di minimo comune multiplo.

Definizione 5.25 *Sia D un dominio e siano $a, b \in D^*$. Si dice che $s \in D$ è un minimo comune multiplo tra a e b e si scrive $s = \mathrm{mcm}(a, b)$ se:*
(i) *s è multiplo sia a che b ($a \mid s \ \ e \ \ b \mid s$).*
(ii) *Per ogni $c \in D \quad a \mid c \ \ e \ \ b \mid c \implies s \mid c$.*

Osservazioni

1. Il massimo comun divisore è unico a meno di fattori unitari. Infatti se d, d' sono due MCD per (ii) $d \mid d'$ e $d' \mid d$. Segue [1] che $d \sim d'$. Inversamente se $d = \mathrm{MCD}(a,b)$ e $d' = ud$ allora $d' = \mathrm{MCD}(a,b)$.
2. Nel caso particolare degli interi il massimo comun divisore è univocamente determinato a meno del segno. Nel caso dei polinomi a meno di costanti non nulle.
3. È facile verificare che un minimo comune multiplo tra due elementi a e b può essere calcolato come
$$\mathrm{mcm}(a,b) = \frac{ab}{\mathrm{MCD}(a,b)}$$

In un dominio euclideo vale una proposizione analoga ad teorema di Bézout (2.6) nel caso degli interi [2].

Teorema 5.31 *Sia D un dominio euclideo con norma ν.*
Dati due elementi $x, y \in D \setminus \{0_D\}$ si consideri la successione

$$z_0 = x; \quad z_1 = y; \quad \dots \quad z_{i+1} = \begin{cases} \textit{Resto divisione di } z_{i-1} \textit{ per } z_i & \textit{se } z_i \neq 0_D \\ 0_D & \textit{se } z_i = 0_D \end{cases}$$

Cioè la successione dei resti ottenuti mediante l'algoritmo delle divisioni successive. Allora esiste un minimo indice n tale che $z_{n-1} = 0_D$ e per tale indice si ha

$$z_n = \mathrm{MCD}(x,y)$$

***D**imostrazione.* Sia la norma $\nu : D \to \mathbb{Z}_0$. Per la definizione della successione, se $z_i \neq 0_D$ allora per un opportuno q_i si ha $z_{i-1} = q_i z_i + z_{n+1}$ con $\nu(z_{i+1}) < \nu(z_i)$. Si ha quindi che la successione degli $\nu(z_i)$ è una successione di interi strettamente decrescente e non negativa. Tale successione non può essere infinita. Quindi esiste un minimo indice $n \in \mathbb{N}$ tale che $z_{n+1} = 0_D$ e poiché $z_0, z_1 \neq 0_D$ deve essere $n > 0$. Consideriamo allora le seguenti uguaglianze:

$$\begin{gathered} z_0 = q_1 z_1 + z_2. \\ z_1 = q_2 z_2 + z_3. \\ \vdots \\ z_{n-2} = q_{n-1} z_{n-1} + \mathbf{z_n}. \\ z_{n-1} = q_n z_n. \end{gathered}$$

Mostriamo che $z_n = \mathrm{MCD}(z_0, z_1)$. Dall'ultima uguaglianza si legge che $z_n \mid z_{n-1}$. Dalla penultima che $z_{n-1} \mid z_{n-2}$ e così via. Ovvero $z_n \mid z_1$ e $z_n \mid z_0$. Supponiamo ora che $a \in D$ sia tale che $a \mid z_0$ e $a \mid z_1$. Allora discendendo si legge che $a \mid (z_0 - q_1 z_1) = z_2$ e così via. Ovvero $a \mid z_n$. ∎

[1] In generale in un dominio due elementi che si dividono a vicenda sono associati. Infatti da $ac = b$ e $b\widetilde{c} = a$ segue che $ac\widetilde{c} = a \;\Rightarrow\; a(c\widetilde{c} - 1) = 0 \;\Rightarrow\; c\widetilde{c} = 1 \;\Rightarrow\; c \in \mathcal{U}$.

[2] In effetti il teorema di Bézout può essere visto come un corollario della seguente proposizione (anche la dimostrazione è simile).

5.8.1 Esempio: divisione di polinomi

Teorema 5.32 *Sia F un campo. Siano $a(x), b(x) \in F[x]$. Sia $b(x) \neq 0$.*
Allora esistono e sono univocamente determinati $q(x), r(x) \in F[x]$ tali che:
(i) $\mathrm{gr}(r(x)) < \mathrm{gr}(b(x))$.
(ii) $a(x) = b(x)q(x) + r(x)$

***D**imostrazione. Esistenza:* procediamo per induzione [1] su $n := \mathrm{gr}(a(x))$.
- Se $n = -1$ allora $a(x) = 0$. Prendendo $q(x) = r(x) = 0$ la (ii) è banalmente verificata in quanto $0 = a(x) = b(x)q(x)+r(x) = 0$. La (i) è verificata: $-1 = \mathrm{gr}(r(x)) < \mathrm{gr}(b(x))$ in quanto $b(x) \neq 0$.
- Supponiamo la tesi vera fino ad un certo $n \geq 0$ e proviamola per n. Si ha $a(x) = a_n x^n + \ldots + a_1 x + a_0$ con $a_n \neq 0$. $b(x)$ sarà quindi della forma $b(x) = b_m x^m + \ldots + b_1 x + b_0$ con $m = \mathrm{gr}(b(x))$ (e quindi $b_m \neq 0$). Se $n < m$ pongo $q(x) = 0$ e $r(x) = a(x)$ e le proprietà sono soddisfatte in automatico.
Se $n \geq m$ consideriamo il polinomio [2]

$$\widetilde{a}(x) := a(x) - a_n b_m^{-1} x^{n-m} b(x) =$$
$$= a(x) - (a_n x^n + a_n b_m^{-1} b_{m-1} x^{n-1} + \ldots + a_n b_m^{-1} b_0 x^{n-m})$$

$\widetilde{a}(x)$ è un polinomio ben definito (F è un campo: *esiste l'inverso moltiplicativo di* b_m) avente grado minore di n poiché i termini di grado n si elidono. Possiamo quindi applicare l'ipotesi induttiva: esistono $\widetilde{q}(x)$, $\widetilde{r}(x) \in F[x]$ tali che $\widetilde{a}(x) = b(x)\widetilde{q}(x) + \widetilde{r}(x)$ con $\mathrm{gr}(\widetilde{r}(x)) < \mathrm{gr}(b(x))$. Si ha quindi

$$a(x) = \widetilde{a}(x) + a_n b_m^{-1} x^{n-m} b(x) = b(x)\widetilde{q}(x) + \widetilde{r}(x) + a_n b_m^{-1} x^{n-m} b(x) =$$
$$= b(x) \cdot (\widetilde{q}(x) + a_n b_m^{-1} x^{n-m}) + \widetilde{r}(x)$$

Quindi ponendo $q(x) := \widetilde{q}(x) + a_n b_m^{-1} x^{n-m}$ e $r(x) := \widetilde{r}(x)$ le proprietà sono verificate. Proviamo ora l'*unicità*. Supponiamo che

$$a(x) = b(x)q(x) + r(x) = b(x)q_1(x) + r_1(x)$$

con $r(x)$ e $r_1(x)$ che $\mathrm{gr}(r(x)) < b$. Segue quindi che

$$b(x)(q(x) - q_1(x)) = r_1(x) - r(x).$$

Se per assurdo $q(x) \neq q_1(x)$ allora $b(x)(q(x) - q_1(x))$ avrebbe grado maggiore di $b(x)$. Allora $\mathrm{gr}(r_1(x) - r(x)) \geq \mathrm{gr}(b(x))$ il che è assurdo in quanto sia $r(x)$ che $r_1(x)$ hanno grado minore di $b(x)$ (e quindi, a maggior ragione, la loro differenza). Allora deve essere necessariamente $q(x) = q_1(x)$. Segue che anche $r(x) = r_1(x)$. ∎

Osservazione Nella dimostrazione precedente l'ipotesi che F sia un campo entra in gioco solo quando si afferma l'esistenza dell'inverso del coefficiente direttivo del polinomio divisore (b_m^{-1}). Quindi il teorema vale nel caso generale di un anello $R[x]$ di polinomi su un anello *commutativo* [3] R in cui però il polinomio $b(x)$ per il quale si divide abbia come coefficiente direttivo un elemento unitario[4].

[1] In seconda forma: assumeremo la tesi vera per $n < n_0$ e la proveremo per $n = n_0$.
[2] In pratica togliamo ad $a(x)$ un polinomio ottenuto mediante $b(x)$ che faccia "sparire" il termine $a_n x^n$ in $a(x)$ abbassando il grado (permettendoci di usare l'ipotesi di induzione).
[3] La commutatività invece è stata usata in larga misura.
[4] Ad esempio in $\mathbb{Z}[x]$ si possono dividere polinomi se e soltanto se il divisore ha $b_m = \pm 1$.

OSSERVAZIONE La procedura usata nella dimostrazione precedente nasconde in realtà anche un metodo per calcolare quoziente e resto tra polinomi. Tale tecnica coincide con la usuale divisione tra polinomi imparata alle scuole inferiori. Infatti se si osserva attentamente ad ogni "passo di induzione" si sottrae ad $a(x)$ un polinomio opportuno ricavato da $b(x)$ che è esattamente il polinomio ottenuto "dividendo" termine $a_n x^n$ per il termine $b_m x^m$ (e in questo punto entra in gioco l'ipotesi di esistenza di b_m^{-1}) e moltiplicando il risultato ottenuto (cioè $a_n b_m^{-1} x^{n-m}$) per $b(x)$. Il quoziente finale è quindi dato dalla somma di tutti i quozienti ottenuti (vedi dimostrazione) e il resto é il dividendo che si ottiene quando si ricade nel caso $n < m$.

ESEMPIO Si vuole calcolare in $\mathbb{Q}[x]$ quoziente e resto tra i polinomi

$$a(x) = 2x^3 + x^2 - 3x + 5 \qquad b(x) = 3x^2 - 2$$

Procedendo come descritto sopra si ottiene:

$+2x^3$	$+x^2$	$-3x$	$+5$	$3x^2-2$
$-2x^3$		$+(4/3)x$		$(2/3)x+1/3$
	x^2	$-(5/3)x$	$+5$	
	x^2		$+2/3$	
		$-(5/3)x$	$+17/3$	

Quindi si ha $q(x) = (2/3)x + 1/3$ e $r(x) = (-5/3)x + 17/3$.

ESEMPIO Se $F = \mathbb{Z}/3\mathbb{Z}$ è il campo delle classi resto modulo 3 si vuole calcolare in $F[x]$ il quoziente e il resto tra i polinomi [5] :

$$a(x) = x^4 + 2x^3 + 2x + 1 \qquad b(x) = 2x^2 + 1$$

Si ottiene quindi (svolgendo i calcoli modulo 3):

$+x^4$	$+2x^3$		$+2x$	$+1$	$2x^2+1$
$-x^4$		$-2x^2$			$2x^2+x-1$
	$+2x^3$	$-2x^2$	$+2x$	$+1$	
	$-2x^3$		$-x$		
		$-2x^2$	$+x$	$+1$	
		$+2x^2$		$+1$	
			x	$+2$	

Quindi si ha $q(x) = 2x^2 + x - 1$ e $r(x) = x + 2$.

In conclusione si ha che se K è un campo *l'anello* $K[x]$ *è un dominio euclideo* rispetto alla norma ν definita dal grado di un polinomio.

[5] Indicando con a_i la classe resto avente come rappresentante a_i.

5.8.2 Esempio: gli interi di Gauss

Sia l'insieme $\mathbb{Z}[i]$ degli *interi di Gauss* definito da:

$$\mathbb{Z}[i] = \{\, x + iy \in \mathbb{C} :\ a, b \in \mathbb{Z} \,\} \quad \text{(Punti a coordinate intere del piano di Gauss)}$$

L'insieme degli interi di Gauss è un dominio euclideo rispetto alla norma ν data dalla norma di un numero complesso:

$$\nu(x + iy) = x^2 + y^2 \in \mathbb{R}^+$$

Infatti la proprietà (i) è banalmente verificata dal fatto che la norma del prodotto di due numeri complessi è pari al prodotto delle loro norme e quindi, in particolare, se $a, b \in \mathbb{Z}[i] \setminus \{\, 0_{\mathbb{C}} \}$ si ha:

$$\nu(ab) = \nu(a)\nu(b) \implies \nu(a) = \frac{\nu(ab)}{\nu(b)} \leq \nu(ab)$$

Per la proprietà (ii) basta osservare [1] che dati $a, b \in \mathbb{Z}[i]$ con $b \neq 0_{\mathbb{C}}$ si ha:

$$ab^{-1} = \xi + \zeta i \qquad \text{(per qualche } \xi, \zeta \in \mathbb{Q})$$

Allora esistono (non necessariamente univocamente determinati) due interi $m, n \in \mathbb{Z}$ che "approssimano" ξ e ζ. Cioè tale che

$$|\xi - m| \leq 1/2 \quad \text{e} \quad |\zeta - n| \leq 1/2$$

Ponendo $\varepsilon i := \xi - m$ e $\eta := \zeta - n$ si ha quindi che

$$a = (\xi + \zeta i)b = ((\varepsilon + m) + (\eta + n)i)b = (m + ni)b + (\varepsilon + \eta i)b$$

Posto $q := m + ni$ e $r := \varepsilon + \eta i$ si vede subito che $r = a - qb \in \mathbb{Z}[i]$ in quanto a, q, b vi appartengono $(m, n \in \mathbb{Z})$. A questo punto se il resto è nullo la condizione (ii) è soddisfatta. Nel caso in cui $r \neq 0$ si ha:

$$\nu(r) = \nu(\varepsilon + \eta i)\nu(b) = (\varepsilon^2 + \eta^2)\nu(b) \leq (1/4 + 1/4)\nu(b) < \nu(b)$$

In particolare $\nu(r) \leq \nu(b)$.

Osservazione Quali sono gli *elementi unitari di* $\mathbb{Z}[i]$?
Se $a, b \in \mathbb{Z}[i]$ sono tali che $ab = 1$ allora passando alle norme si ottiene:

$$ab = 1 \implies \nu(ab) = \nu(a)\nu(b) = \nu(1) = 1$$

E quindi deve essere $\nu(a) = \nu(b) = 1$. Gli elementi unitari di $\mathbb{Z}[i]$ possono quindi essere soltanto $1, -1, i, -i$. Tali elementi sono unitari (e quindi gli unici elementi unitari di $\mathbb{Z}[i]$) perché $1 \cdot 1 = 1,\ (-1) \cdot (-1) = 1,\ i \cdot (-i) = 1$.

Per calcolare il quoziente tra due interi di Gauss a, b si procede come visto sopra: si calcola la quantitá ab^{-1} e si svolgono i calcoli [2] fino ad ottenere $ab^{-1} = \xi + \zeta i$ per una coppia ξ, ζ di razionali. A questo punto si prende come quoziente l'intero più vicino a ξ e come resto l'intero più vicino a ζ. Ovviamente se ξ o ζ valgono $1/2$ quoziente e resto non saranno unici.

[1] Ricordando che se $z \in \mathbb{C}$ il suo inverso è dato da $z^{-1} = \overline{z}/|z|^2$ ($\overline{z}$ = coniugato di z).
[2] Tipicamente risulta efficace procedere come: $ab^{-1} = a/b = a/b \cdot \overline{b}/\overline{b} = \ldots = \xi + \zeta i$.

Esempi

1. Calcolare quoziente e resto tra $x = 4 + 3i$ e $2 + i$.

$$\frac{4+3i}{2+i} = \frac{(4+3i)(2-i)}{(2+i)(2-i)} = \frac{8+6i-4i+3}{5} = \frac{11}{5} + \frac{2}{5}i \;\approx\; 2 + 0i = 2$$

   Il quoziente è quindi 2 e il resto è dato da $4 + 3i - 2 \cdot (2 + i) = i$.

2. Calcolare MCD$(4 + 2i,\, 5 + 3i)$. La procedura standard è fornita dalla versione generale del teorema di Bézout (teorema 5.31) e consiste nel procedere per divisioni successive fino a determinare l'ultimo resto non nullo. Quindi si ha $\nu(4 + 2i) = 16 + 4 = 20$; $\nu(5 + 3i) = 25 + 9 = 34$. Dividiamo l'elemento di norma maggiore per quello di norma minore.

$$\frac{5+3i}{4+2i} \cdot \frac{4-2i}{4-2i} = \frac{20+12i-10i+6}{20} = \frac{26}{20} + \frac{2}{20}i \;\approx\; 1 + 0 \cdot i$$

   Il quoziente è quindi 1 e il resto è $5 + 3i - 1 \cdot (4 + 2i) = 1 + i \neq 0$. Dividendo $4 + 2i$ per il resto si ottiene:

$$\frac{4+2i}{1+i} \cdot \frac{1-i}{1-i} = 3 - i$$

   Il resto è ora $4 + 2i - (3 - i)(1 + i) = 0$. Quindi abbiamo finito e il massimo comun divisore è l'ultimo resto non nullo: $1 + i$.

Osservazione Quali sono gli *elementi primi in* $\mathbb{Z}[i]$? Gli interi primi in $\mathbb{Z}$ sono primi in $\mathbb{Z}[i]$? La risposta alla seconda domanda è no. Ad esempio

$$2 = (1 + i)(1 - i)$$

è un primo di $\mathbb{Z}$ che si scrive come prodotto (non banale) di due primi $1 + i$ e $1 - i$. Quindi non essendo irriducibile non può essere primo (per 5.27). Se $p \in \mathbb{Z}$, $p \neq 2$ è un numero primo allora è congruo a 1 o a -1 modulo 4. Quello che si può dimostrare è che i numeri primi che sono congrui a -1 modulo 4 sono primi anche in $\mathbb{Z}[i]$. Tali numeri sono tutti e soli i numeri che si possono esprimere come somma di due quadrati.

5.9 Domini a fattorizzazione unica

Definizione 5.26 (UFD) *Un dominio di integrità D si dice a fattorizzazione unica, e si abbrevia dicendo che D è* UFD *(unic factorization domain), se:*
(i) *Ogni $a \in D$, $a \neq 0_D$* non unitario *è prodotto di $r \geq 1$ elementi (fattori) irriducibili.*
(ii) *Date due fattorizzazioni $a = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$ in fattori irriducibili allora $s = t$ e a meno di un eventuale riordinamento $p_i = u_i q_i$ per alcuni $u_1, \dots, u_s \in \mathcal{U}$ (i.e. i fattori delle due fattorizzazioni sono associati).*

Definizione 5.27 *Se D è un dominio diremo che:*

(CP) *D gode della* condizione di primalità *se ogni elemento irriducibile è primo.*

(CC) *D gode della* condizione di catena sui divisori *se non contiene alcuna sequenza* infinita *di elementi $a_1, a_2, \dots, a_i, \dots$ in cui $\forall\, i$ a_{i+1} sia un fattore proprio di a_i. Equivalentemente data una sequenza $a_1, a_2, \dots$ in cui $\forall\, i$, $a_{i+1} \mid a_i$ allora esiste un indice n_0 a partire dal quale tutti gli a_i sono associati ($a_{n_0} \sim a_{n_0+1} \sim \dots$).*

(CC') *D gode della* condizione di catena sugli ideali principali *se non esiste alcuna catena strettamente ascendente* infinita *di ideali principali*

$$(a_1) \subset (a_2) \subset \dots (a_i) \subset (a_{i+1}) \subset \dots$$

Osservazione Si osservi che le condizioni di catena sui divisori e sugli ideali sono equivalenti in quanto, come osservato a pagina 77, un elemento b é un fattore proprio di a se e solo se $(a) \subset (b) \subset D$.

Teorema 5.33 (UFD $\Rightarrow$ CP)
Sia D un dominio UFD. *Allora in D vale la* CP.
In particolare in un UFD *un elemento è primo se e solo se è irriducibile.*

***D**imostrazione.* Sia p un irriducibile in D e supponiamo che $p \mid ab$ $(a, b \in D)$. Allora $ab = pc$ per qualche $c \in D$. La tesi è ovvia se a o b sono nulli. Sia quindi $a, b \neq 0_D$.
- Se a è unitario posso scrivere $b = p(a^{-1}c)$ e dunque $p \mid b$.
Similmente nel caso in cui b è unitario $p \mid a$.
- Se né a né b sono unitari ($a, b \notin \mathcal{U}$) allora, essendo D un UFD, a e b si scrivono come prodotto di fattori irriducibili:

$$a = p_1 p_2 \dots p_s \qquad b = q_1 q_2 \dots q_t \qquad ab = p_1 p_2 \dots p_s q_1 q_2 \dots q_t \notin \mathcal{U}$$

Allora $p \mid ab$ implica $pc = ab$ e per l'unicità di fattorizzazione (p è irriducibile) p deve essere associato a qualche p_i o a qualche q_j. Nel primo caso $p \mid a$, nel secondo $p \mid b$. ∎

Teorema 5.34 (UFD $\Rightarrow$ CC)
Sia D un UFD. *Allora vale la condizione di catena sui divisori* CC.

***D**imostrazione.* Sia $a_1 \in D$. Se a è unitario ogni sequenza di fattori non può essere che composta da fattori associati. Se $a_1 \notin \mathcal{U}$ non é unitario allora sia $a_1 = p_1 \dots p_{r_1}$ la sua scomposizione in fattori irriducibili. Allora a_2 deve essere un fattore proprio di a_1 e quindi deve avere lunghezza minore di r_1; diciamo r_2. In generale ad una qualsiasi catena $\{ a_1, a_2, \dots \}$ è associata una successione $\{ r_1, r_2, \dots \}$ strettamente decrescente. Esiste quindi un indice n_0 a partire dal quale la lunghezza è pari ad 1. Allora $\forall\, n \geq n_0,\ a_n \sim a_{n+1}$. ∎

Vale anche il viceversa: se in un dominio D vale la condizione di catena allora si prova l'esistenza di una fattorizzazione in irriducibili. Se inoltre vale la condizione di primalità allora tale fattorizzazione è unica a meno di fattori unitari.

Teorema 5.35 *Sia D un dominio.*
D è UFD $\iff$ *valgono* (CP) *e* (CC).

***D**imostrazione.* Proviamo che *la condizione di catena implica l'esistenza di una fattorizzazione in irriducibili.* Sia $a \neq 0_D,\ a \notin \mathcal{U}$. Se a è irriducibile ho finito.
Altrimenti posso scrivere $a = a_1 b_1$ con a_1 fattore proprio di a.

$$\begin{array}{c} a_1 \text{ è irriducibile oppure } a_1 = a_2 b_2 \text{ con } a_2 \text{ fattore proprio di } a_1. \\ a_2 \text{ è irriducibile oppure } a_2 = a_3 b_3 \text{ con } a_3 \text{ fattore proprio di } a_2. \\ \ldots \quad . \quad \ldots \end{array}$$

Si ha quindi una catena $\{ a_1, a_2, \ldots \}$ che, in forza della condizione (CC), deve terminare con un elemento a_n irriducibile. Poniamo $p_1 := a_n$. Si ha che $a = p_1 a'$.

$$\begin{array}{c} \text{Lo stesso discorso fatto per } a' \text{ produce un irriducibile } p_2 \text{ tale che } a' = p_2 a''. \\ \text{Lo stesso discorso fatto per } a'' \text{ produce un irriducibile } p_3 \text{ tale che } a'' = p_3 a'''. \\ \ldots \quad . \quad \ldots \end{array}$$

Si ottiene quindi una catena $\{ a, a', a'', \ldots, a^{(i)}, \ldots \}$ in cui $a^{(i+1)} = a^{(i)} p_i$.
Sempre in virtù di (CC) anche questa sequenza deve terminare con un elemento irriducibile $p_t := a^{(t-1)}$. Si conclude che:

$$a = p_1 a' = p_1 p_2 a'' = \ldots = p_1 p_2 \ldots p_t$$

E l'esistenza è provata. Proviamo che *la condizione di primalità implica l'unicità di fattorizzazione.* Siano $a = p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_t$ due fattorizzazioni di a in irriducibili. Procediamo per induzione sul numero dei fattori s.
- Se $s = 1$ allora $a = p_1$ è irriducibile. Segue che $t = 1$ e che $p_1 = q_1$ in quanto non possono avere altri fattori.
- Se $s > 1$ poiché $p_1(p_2 \ldots p_s) = q_1 q_2 \ldots q_t \implies p_1 \mid (q_1 q_2 \ldots q_t)$ Essendo p_1 irriducibile per la (CP) è primo. Allora esiste un indice j tale che $p_1 \mid q_j$. A meno di riordinare i fattori (D è commutativo) possiamo supporre $j = 1$. Allora, essendo q_1 e p_1 irriducibili, si ha che $p_1 \mid q_1 \implies p_1 \sim q_1$. Quindi $q_1 = u p_1$ con $u \in \mathcal{U}$. Quindi

$$p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_t = u p_1 q_2 \ldots q_t \implies p_2 \ldots p_s = q_2' \ldots q_t$$

Dove si è posto $q_2' = u q_2$. Essendo q_2' a sua volta un irriducibile per ipotesi induttiva si ha che $s - 1 = t - 1 \implies s = t$ e a meno di un riordinamento $p_i \sim q_i\ \forall\, i = 2, \ldots, s$. Avendo inoltre provato che $p_1 \sim q_1$ segue l'unicità di scrittura. ■

Definizione 5.28 *Diremo che in un dominio D vale la condizione di esistenza del massimo comun divisore (e abbrevieremo dicendo che D ha la* CM*) se per ogni coppia di elementi non nulli esiste un massimo comun divisore.*

Teorema 5.36 **(**UFD $\Rightarrow$ CM**)**
In un dominio UFD *per ogni $a, b \in D^*$ esiste* MCD(a, b).

***D**imostrazione.* Siano $a, b \neq 0_D$. Se uno dei due è unitario allora [1] divide ogni altro e quindi è un massimo comun divisore. Possiamo quindi supporre $a, b \notin \mathcal{U}$. Consideriamo allora una fattorizzazione di a. Se alcuni fattori $p_{i_1} \sim p_{i_2} \sim \ldots \sim p_{i_e}$

[1] Per quanto osservato a pagina 76.

sono associati possiamo scrivere $p_{i_1}p_{i_2}\dots p_{i_e} = up_{i_1}^e =: up_i^e$ in modo da raggruppare nella fattorizzazione di a i fattori associati ed ottenere una fattorizzazione

$$a = u \cdot p_1^{e_1} \dots p_r^{e_r} \qquad \text{con } u \in \mathcal{U} \text{ e } p_1^{e_1}, \dots, p_r^{e_r} \text{ non associati.}$$

In modo analogo è possibile scrivere $b = u' p_1^{g_1} \dots p_t^{g_t}$ con $u \in \mathcal{U}$ e i rimanenti fattori non associati. È possibile cioè immaginare che ci sia la stessa scrittura formale a patto di mettere $g_i = 0$ ad eventuali $p_i^{g_i}$ che non compaiono. Se ora per ogni $i = 1, \dots, t$ poniamo $h_i := \min(e_i, g_i)$ e chiamiamo $d := p_1^{h_1} \dots p_t^{h_t}$ si ha che chiaramente d soddisfa le proprietà del massimo comun divisore (per costruzione è il massimo fattore in comune). ∎

Ogni dominio a ideali principali è a fattorizzazione unica. D'altra parte, per il teorema 5.30, ogni dominio euclideo è a ideali principali. Segue che ogni dominio euclideo è a fattorizzazione unica. Proviamo quindi la prima affermazione:

Teorema 5.37 (PID $\Rightarrow$ UFD**)**
Ogni PID *è un* UFD*.*

D*imostrazione.* Sia D un PID. Proviamo che valgono (CP) e (CC).
Vale la condizione d primalità. Sia p un irriducibile. Supponiamo che $p \mid ab$. Dobbiamo mostrare che se $p \nmid a$ allora $p \mid b$ (e quindi p è primo). Poiché p è irriducibile [2] *non* esiste alcun ideale J di D tale ch e $(p) \subset J \subset D$. D'altra parte si ha che l'elemento a non sta in (p) (se così fosse dovrebbe essere $p \mid a$ il che è falso per ipotesi). Quindi, ponendo $J := (a) + (p)$ (ideale somma) deve essere necessariamente

$$(a) + (p) = D$$

In particolare $(a) + (p)$ deve contenere l'unità. Quindi per opportuni $x, y \in D$ deve essere $1_D = xa + yp \implies b = xab + ypb$. Dal fatto che $p \mid ab$ segue che $pc = ab$ per qualche $c \in D$. Ma allora

$$b = xpc + ypb = p(xc + yb) \implies p \mid b$$

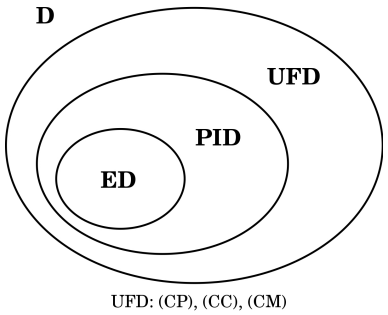
Quindi p è primo. Proviamo che *vale la condizione di catena sugli ideali principali* (CC′). Sia dunque $(a_1) \subset (a_2) \subset \dots$ una catena strettamente ascendente si ideali principali[3]. Allora essendo $\{ (a_i) \}_i$ una catena ascentente si ha che

$$I := \bigcup_i (a_i) \qquad \text{è un ideale di } D.$$

Ma siccome D è a ideali principali $I = (d)$ è principale. Quindi d sta in qualche (a_n) per un opportuno n. Da $I = (d) \subseteq (a_n)$ e $(a_n) \subseteq I$ segue che $I = (a_n)$. Allora la catena non può essere infinita in quanto (a_{n+1}) dovrebbe contenere propriamente I e allo stesso tempo essere contenuto in I. ∎

[2] Si veda quanto osservato a pagina 77.
[3] D è un UFD. Ogni ideale in D è principale.

OSSERVAZIONE Possiamo sintetizzare la posizione reciproca di un ED, PID e UFD con la seguente figura:



OSSERVAZIONE È possibile dimostrare che *se in un dominio vale la* (CM) *allora vale anche la* (CP). Cioè se in un dominio per ogni coppia di elementi non nulli esiste un massimo comun divisore allora ogni elemento irriducibile è primo. È allora possibile riformulare (in forza dei teoremi 5.33, 5.34 e 5.36) il teorema 5.35 dicendo che un dominio D è UFD $\iff$ valgono (CM) e (CC).

Proposizione 5.38 *Sia D un dominio a ideali principali.*
Siano $a, b \in D^* = D \setminus \{0_D\}$. Allora:
(i) $(a, b) = Da + Db = (d)$ *ove* $d = \text{MCD}(a, b)$.
(ii) $(a) \cap (b) = (t)$ *ove* $t = \text{mcm}(a, b)$.

***D**imostrazione.* In un UFD esistono $\text{MCD}(a, b)$ ed $\text{mcm}(a, b)$.
(i) Essendo D un PID si ha $(a, b) = (d)$. Allora essendo $a, b \in (D)$ si ha che $d \mid a$ e $d \mid b$. D'altronde $d = xa + yb$ con opportuni $x, y \in D$. Pertanto se $c \mid a$ e $c \mid b$ allora $c \mid d$. Segue che $d \sim \text{MCD}(a, b)$ è un massimo comun divisore.
(ii) Sia $(a) \cap (b) = (t)$ (l'intersezione di due ideali è un ideale; principale perché D è un PID). Quindi $t \in (a)$ e $t \in (b)$ implica $a \mid s$ e $b \mid s$. Essendo $s \in (t)$ si ha $t \mid s$. Quindi t è un minimo comune multiplo. ■

In particolare l'ideale (a, b) è tutto D se e solo se a e b sono coprimi. Quindi la proposizione precedente giustifica, nel caso di un PID, la seguente definizione:

Definizione 5.29 *Sia R un anello. Due ideali si dicono coprimi se $I + J = R$.*

5.10 Teorema cinese dei resti

Teorema 5.39 (Teorema cinese dei resti)
Sia R un anello commutativo *e siano $J_1, \ldots, J_n$ ideali di R a due a due coprimi (i.e. $J_i + J_j = R$ se $i \neq j$). Per $i = 1, \ldots n$ sia $\pi_i : R \to R/J_i$ l'epimorfismo canonico. Sia $\varphi : R \to R/J_1 \times \ldots \times R/J_n$ (anello prodotto) l'applicazione definita ponendo*

$$\forall\, x \in R \qquad \varphi(x) := (\pi_1(x),\ \ldots,\ \pi_n(x))$$

Allora questa mappa è un morfismo suriettivo *di anelli avente nucleo $\bigcap_{i=1}^{n} J_i$.*
In particolare per il teorema d'omomorfismo si ha [1]*:*

$$R/\bigcap_{i=1}^{n} J_i \backsimeq \prod_{i=1}^{n} R/J_i$$

***D**imostrazione.* Le proiezioni π_i sono morfismi per ogni i. Quindi il fatto che φ sia un morfismo segue da come sono definite le operazioni nell'anello prodotto (vedi def. 5.7). $x \in \ker\varphi$ se $\varphi(x) = \underline{0} = (J_1,\ \ldots,\ J_n)$ e ciò avviene se e solo se $x \in J_1,\ \ldots,\ x \in J_n$ cioè se e solo se $x \in \bigcap_{i=1}^{n} J_i$. Quindi φ ha come nucleo tale intersezione.
Proviamo che φ è suriettiva. Cominciamo con provare che

$$\forall\, i = 1,\ \ldots,\ n \qquad J_i + \bigcap_{k \neq i} J_k = R \qquad \textit{(i.e. sono coprimi)}$$

Per ipotesi $\forall\, k \neq i$ si ha $J_i + J_k = R$. In particolare se $i \neq k$ esistono $a_i \in J_i$ e $a_k \in J_k$ tale che $a_i + a_k = 1_R$. Moltiplicando queste quantità al variare di $i \neq k$ e usando la distributività si ottiene che

$$1_R = \prod_{i \neq k}(a_i + a_k) \ \in\ J_i + \prod_{i \neq k} J_k \ \subseteq\ J_i + \bigcap_{i \neq k} J_k$$

Tale ideale, dovendo contenere l'unità, deve essere quindi l'intero anello. In particolare per ogni $i = 1,\ \ldots,\ n$ devono esistere $d_i \in J_i$ ed $e_i \in \bigcap_{k \neq i} J_k$ tale che

$$d_i + e_i = 1_R$$

Se $i \neq j$ allora, essendo $\ker\pi_j = J_j$, si ha che $\pi_j(e_i) = \underline{0}$ in quanto $e_i \in J_j$.
Se $i = j$ allora $d_i + e_i = 1_R \implies \pi_i(d_i) + \pi_i(e_i) = \underline{0} + \pi_i(e_i) = \pi_i(1_R) = \underline{1}$.
Quindi si ha che $\pi_j(e_i) = \delta_{ij}$. A questo punto è immediato provare la suriettività. Sia $(y_1, \ldots, y_n) \in \prod_{i=1}^{n} R/J_i$. Per ogni $i = 1, \ldots, n$ sia $x_i \in \pi_i^{-1}(y_i)$. Allora una preimmagine di $(y_1, \ldots, y_n)$ è data da:

$$x := \sum_{i=1}^{n} x_i e_i$$

Infatti

$$\varphi(x) = \sum_{i=1}^{n} \varphi(x_i)\varphi(e_i) = \sum_{i=1}^{n} (\pi_1(x_i),\ \ldots,\ \pi_n(x_i)) \cdot (\pi_1(e_i),\ \ldots,\ \pi_n(e_i)) =$$

$$= \sum_{i=1}^{n} (\,\underline{0}\,,\ \ldots,\ \pi_i(x_i),\ \underline{0}\,,\ \ldots,\ \underline{0}\,) = (y_1,\ \ldots,\ y_n)$$

E questo conclude la dimostrazione. ∎

[1] Indicando con il simbolo di produttoria il prodotto cartesiano di n insiemi.

Definizione 5.30 *Sia R un anello* commutativo. *Sia J un ideale di R.*
$x, y \in R$ si dicono congrui modulo J se $x - y \in J$ ovvero se

$$J + x = J + y$$

Se x e y sono congrui modulo J scriveremo $x \equiv y \ _{(J)}$.
Se poi $J = (a) = Ra$ allora scriveremo $x \equiv y \ _{(a)}$.

OSSERVAZIONE La definizione appena data di elementi congrui coincide con la definizione usuale nel caso in cui $R = \mathbb{Z}$ e $J = (n) = n\mathbb{Z}$. Infatti in tal caso due numeri x, y sono cogrui modulo n se e solo se $[\, x \,]_n = [\, y \,]_n$ cioè se e solo se $n\mathbb{Z} + x = n\mathbb{Z} + y$.

Il Teorema cinese dei resti si può riformulare nel modo seguente:

Corollario 5.40 *Sia R un anello commutativo e siano $J_1, \ldots, J_n$ ideali di R.*
Allora assegnati $x_1, \ldots, x_n \in R$ esiste sempre $x \in R$ tale che:

$$\forall\, i = 1, \ldots, n \qquad x \equiv x_i \ _{(J_i)}$$

***D**imostrazione.* Data una n-upla $(J_1 + x_1, \ \ldots, \ J_n + x_n)$, per la suriettività di φ esiste una preimmagine x. Esiste cioè $x \in R$ tale che

$$\varphi(x) = (\pi_1(x), \ \ldots, \ \pi_n(x)) = (J_1 + x, \ \ldots, \ J_n + x) = (x_1, \ \ldots, \ x_n)$$

Cioè esiste $x \in R$ tale che $x \equiv x_i \ _{(J_i)}$ per ogni $i = 1, \ldots, n$. ∎

Corollario 5.41 *Siano $a_1, \ \ldots, \ a_n \in \mathbb{Z}$ a due a due coprimi.*
Allora assegnati comunque n interi $x_1, \ \ldots, \ x_n \in \mathbb{Z}$ il sistema di congruenze lineari:

$$\begin{cases} x \equiv x_1 \ _{(a_1)} \\ \quad \vdots \\ x \equiv x_n \ _{(a_n)} \end{cases}$$

ha sempre soluzione in $\mathbb{Z}$. Se $\widetilde{x}$ è una soluzione particolare del sistema ogni altra soluzione è congrua a $\widetilde{x}$ modulo $a_1 \ldots a_n$.

***D**imostrazione.* Basta osservare che gli ideali principali $(a_1), \ \ldots, \ (a_n)$ sono a due a due coprimi se e solo se $a_1, \ldots, a_n$ lo sono. Inoltre se $\widetilde{x}$ e $\widetilde{x}'$ sono soluzioni allora $\pi_\varphi : R \to R/\bigcap_{i=1}^n J_i$ manda entrambe le soluzioni nello stesso elemento in quanto hanno la stessa immagine mediante φ. Segue che, posto $I := \bigcap_{i=1}^n J_i$, si ha $I + \widetilde{x} = I + \widetilde{x}'$. Cioè che le soluzioni sono congruenti modulo

$$\bigcap_{i=1}^{n} J_i = \bigcap_{i=1}^{n} (a_i) = (\mathrm{mcm}(a_1, \ldots, a_n)) = (a_1 \ldots a_n)$$

Che è quanto si voleva provare. ∎

La dimostrazione del Teorema cinese dei resti suggerisce anche un metodo per risolvere sistemi di congruenze. Ad esempio supponiamo di lavorare in $\mathbb{Z}$ e di voler risolvere il sistema

$$\begin{cases} x \equiv b_1 \ _{(n_1)} \\ \quad \vdots \\ x \equiv b_n \ _{(n_r)} \end{cases}$$

Allora, se $\text{MCD}(n_i, n_j) = 1$ ogni volta che $i \neq j$, possiamo applicare il teorema e dire che il sistema ammette soluzioni e se c_0 è una soluzione particolare allora ogni altra soluzione è della forma $c = c_0 + kN$ dove $N := n_1 \dots n_r = \text{mcm}(n_1, \dots, n_r)$. Quindi il problema si riduce a trovare una soluzione particolare c_0.

La dimostrazione del teorema fornisce un modo per trovare tale soluzione. Infatti se per ogni i chiamiamo $N_i := N/n_i$ il generatore dell'ideale $(N_i) = \bigcap_{j \neq i}(n_j)$ allora dalla dimostrazione sappiamo che per ogni i esistono $d_i \in (n_i)$ e $e_i \in (N_i)$ tali che $d_i + e_i = 1$. Una volta trovati gli e_i una soluzione particolare è data da:

$$c_0 = \sum_{i=1}^{r} b_i e_i$$

Per trovare gli e_i notiamo che un generico $d_i \in (n_i)$ è della forma $d_i = n_i t$ e un generico $e_i \in N_i$ è della forma $e_i = N_i y_i$ per qualche $t, y_i \in R$. Quindi

$$d_i + e_i = 1 \iff n_i t + N_i y_i = 1 \iff N_i y_i - 1 = -t n_i \iff N_i y_i \equiv 1 \ _{(n_i)}$$

Si noti che tale congruenza in generale ammette sempre soluzione perché avviene sempre che $1 = \text{MCD}(N_i, n_i) \mid 1$. Quindi per trovare la soluzione c_0 basta risolvere le r congruenze lineari e trovare $y_1, \dots, y_r$. La soluzione sarà quindi:

$$c_0 = b_1 N_1 y_1 + b_2 N_2 y_2 + \dots + b_r N_r y_r.$$

Esempi

1. Consideriamo il sistema
$$\begin{cases} x \equiv 2 \ _{(3)} \\ x \equiv 3 \ _{(5)} \\ x \equiv 2 \ _{(7)} \end{cases}$$
Essendo n_1, n_2, n_3 coprimi posso applicare il teorema cinese.
Si ha $N = 3 \cdot 5 \cdot 7 = 105$. La soluzione sarà $c = c_0 + k \cdot 105$.
Determino c_0.

   1) $N_1 = N/n_1 = 5 \cdot 7 = 35$. Devo risolvere:
   $$N_1 y_1 \equiv 1 \ _{(n_1)} \implies 35 y_1 \equiv 1 \ _{(3)} \implies 2 y_1 \equiv 1 \ _{(3)} \implies y_1 \equiv 2 \ _{(3)}$$
   Ad esempio posso prendere $y_1 = 2$.
   2) $N_2 = N/n_2 = 3 \cdot 7 = 21$. Devo risolvere:
   $$N_2 y_2 \equiv 1 \ _{(n_2)} \implies 21 y_2 \equiv 1 \ _{(5)} \implies y_2 \equiv 1 \ _{(5)}$$
   Ad esempio posso prendere $y_2 = 1$.
   3) $N_3 = N/n_3 = 3 \cdot 5 = 15$. Devo risolvere:
   $$N_3 y_3 \equiv 1 \ _{(n_3)} \implies 15 y_3 \equiv 1 \ _{(7)} \implies y_3 \equiv 1 \ _{(7)}$$
   Ad esempio posso prendere $y_3 = 1$.

   Allora una soluzione particolare è data da
   $$c_0 = b_1 N_1 y_1 + b_2 N_2 y_2 + b_3 N_3 y_3 = 140 + 63 + 30 = 233$$
   Quindi prendendo la minima soluzione positiva si ha $c = 23 + k \cdot 105$. È di solito opportuno un controllo del risultato: $23 - 2 \mid 3,\ 23 - 3 \mid 5,\ 23 - 2 \mid 7$. Ook.

2. Consideriamo il sistema

$$\begin{cases} 3x \equiv 2 \ _{(3)} \\ 5x \equiv 7 \ _{(12)} \\ 3x \equiv 1 \ _{(7)} \end{cases} \iff \begin{cases} x \equiv 4 \ _{(3)} \\ x \equiv 11 \ _{(12)} \\ x \equiv 5 \ _{(7)} \end{cases}$$

Essendo n_1, n_2, n_3 coprimi posso applicare il teorema cinese.
Prima di applicare il teorema è necessario però avere i coefficienti dell'incognita x pari ad 1. Si ha $N = 5 \cdot 12 \cdot 7 = 420$. La soluzione sarà $c = c_0 + k \cdot 420$.
Determino c_0.

1) $N_1 = N/n_1 = 12 \cdot 7 = 84$. Devo risolvere:

$$84y_1 \equiv 1 \ _{(5)} \implies 4y_1 \equiv 1 \ _{(5)} \implies y_1 \equiv -1 \ _{(3)}$$

Ad esempio posso prendere $y_1 = -1$.

2) $N_2 = N/n_2 = 5 \cdot 7 = 35$. Devo risolvere:

$$11y_2 \equiv 1 \ _{(12)} \implies y_2 \equiv -1 \ _{(12)}$$

Ad esempio posso prendere $y_2 = -1$.

3) $N_3 = N/n_3 = 12 \cdot 5 = 60$. Devo risolvere:

$$60y_3 \equiv 1 \ _{(7)} \implies 4y_3 \equiv 1 \ _{(7)} \implies y_3 \equiv 2 \ _{(7)}$$

Ad esempio posso prendere $y_3 = 2$.

Allora una soluzione particolare è data da

$$c_0 = b_1 N_1 y_1 + b_2 N_2 y_2 + b_3 N_3 y_3 = -121$$

Quindi prendendo la minima soluzione positiva si ha $c = 299 + k \cdot 420$.

Se $n_1, \ldots, n_r$ non sono a due a due coprimi in generale non è possibile usare il teorema cinese dei resti. È però possibile usare la seguente estensione nel caso di $\mathbb{Z}$:

Teorema 5.42 *Sia dato il seguente sistema di congruenze lineari in $\mathbb{Z}$:*

$$\begin{cases} x \equiv b_1 \ _{(n_1)} \\ \quad \vdots \\ x \equiv b_r \ _{(n_r)} \end{cases}$$

Allora il sistema ammette soluzione se e solo se $\forall\, i \neq j$ si ha $\mathrm{MCD}(n_i, n_j) \mid (b_i - b_j)$. *In tal caso la soluzione è* $c = c_0 + k \cdot \mathrm{mcm}(n_1, \ldots, n_r)$.

Esempi

1. Supponiamo di voler risolvere il sistema

$$\begin{cases} x \equiv 7 \ _{(9)} \\ x \equiv 10 \ _{(15)} \end{cases}$$

Verifichiamo che ammetta soluzione: $\mathrm{MCD}(9, 15) = 3 \mid (9 - 15) = -3$. Per risolvere il sistema procediamo per via diretta. Dalle congruenze si deduce che:

$$\begin{aligned} x \equiv 7 \ _{(9)} &\iff 9u = x - 7 \\ x \equiv 10 \ _{(15)} &\iff 15v = x - 10 \end{aligned}$$

Quindi si ha $x = 7 + 9u = 10 + 15v \implies 9u - 15v = 3$. Dividendo per 3 si ottiene la seguente equazione diofantea: $3u - 5v = 1$. Delle soluzioni si possono trovare facilmente: $u = -3,\ v = -2$. Quindi si ha $x = 7 - 27 = -20$. Allora $c = -20 + k \cdot \text{mcm}(9, 15) = -20 + k \cdot 45$.

2. Supponiamo di voler risolvere il sistema

$$\begin{cases} x \equiv 5 \ _{(6)} \\ x \equiv 8 \ _{(15)} \\ x \equiv 3 \ _{(10)} \end{cases}$$

$\text{MCD}(9, 15) = 3 \mid (5 - 8);\ \text{MCD}(6, 10) = 2 \mid (5 - 3);\ \text{MCD}(15, 10) = 5 \mid (8 - 3);$. Le soluzioni sono quindi della forma $c = c_0 + k \cdot \text{mcm}(6, 15, 10) = c_0 + k \cdot 30$. Cominciamo con il risolvere il sottosistema:

$$\begin{cases} x \equiv 5 \ _{(6)} \\ x \equiv 8 \ _{(15)} \end{cases}$$

Dalle congruenze si deduce che $x = 6u + 5 = 8 + 15v \implies 6u - 15v = 3 \implies 2u - 5v = 1$. Ad esempio $u = 3$ e $v = 1$. Quindi la soluzione di questo sottosistema è $x = 23 + k \cdot \text{mcm}(6, 15) = 23 + k \cdot 30$. Quindi sostituendo la soluzione alle due congruenze si ottiene il seguente sistema:

$$\begin{cases} x \equiv 23 \ _{(30)} \\ x \equiv 3 \ _{(10)} \end{cases}$$

Da cui si ottiene $x = 10v + 3 = 30u + 23 \implies 10v - 30u = 20 \implies v - 3u = 2$. Ad esempio $u = 1$ e $v = 5$. Quindi si ha $c = 53 + k \cdot 30$.

5.11 Radici di polinomi

Se X è un insieme non vuoto ed A è un anello allora $A^X = \{ f : X \to A \}$ ha una naturale struttura di anello rispetto alle operazioni:

$$\forall\, f, g \in A^X \qquad (f+g)(x) := f(x) + g(x) \qquad (fg)(x) := f(x)g(x)$$

In questo modo si ha una struttura di anello in cui l'unità è l'applicazione $f(x) = 1_A$ che associa ad ogni $x \in X$ l'unità dell'anello A e lo zero è l'applicazione nulla $f(x) = 0_A$. Se $X = \{ 1, \ldots, n \}$ allora $A^X \backsimeq A^n$ tramite l'identificazione (immagine)-(n-upla).

Definizione 5.31 *Sia $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in A[x]$.*
Definiamo $F \in A^A$ ponendo $\forall\, \alpha \in A$:

$$F(\alpha) := a_n \alpha^n + \ldots + a_1 \alpha + a_0 \in A$$

F si dice funzione polinomiale associata *ad $f(x)$. Per abuso di notazione se $f(x) \in A[x]$ indicheremo la funzione F associata ancora con il simbolo $f(x) \in A^A$.*

Lemma 5.43 *L'applicazione $\Phi : A[x] \to A^A$ che associa ad ogni polinomio la sua funzione polinomiale associata è un morfismo di anelli.*

Osservazioni

1. L'omomorfismo Φ non è in generale iniettivo. Ció accade certamente se A è un anello finito. Infatti A finito $\Leftrightarrow A^A$ finito. Quindi, essendo $A[x]$ infinito, il morfismo Φ non può essere iniettivo. Se invece A è un dominio di integrità di caratteristica 0 allora Φ è iniettiva.
2. Se $A \subseteq B$ è un'*estensione di anelli* (i.e. A, B anelli con $A \subseteq B$) allora anche $A[x] \subseteq B[x]$ è un'estensione di anelli. Per ogni $f(x) \in A[x]$ e $b \in B$ possiamo valutare f in B e considerare $f(b) \in B$. Quindi per ogni $b \in B$ è definita la funzione V_b come:

   $$V_b : A[x] \to B \qquad f(x) \longmapsto f(b) \qquad \textit{(Omomorfismo di valutazione)}$$

   Tale applicazione è un morfismo di anelli.
3. Se $A = \mathbb{Z}/p\mathbb{Z}$ con p primo allora il polinomio $f(x) = x^p - x = x(x^{p-1} - 1)$ ha funzione polinomiale associata nulla anche se non è il polinomio nullo. Infatti per il piccolo teorema di Fermat $[\, a \,]_p^{p-1} = [\, a \,]_p^{\phi(p)} = [\, 1 \,]_p$
4. In generale in ogni anello commutativo A l'espressione $(a \pm b)^n$ si può calcolare con la usuale formula di Newton-Leibniz:

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

   In particolare se $A = \mathbb{Z}/p\mathbb{Z}$ con p primo allora $(a \pm b)^p = a^p \pm b^p$ in quanto il coefficiente $\binom{n}{k}$ è un multiplo di p (e quindi nullo modulo p).

Definizione 5.32 *Sia A un anello commutativo e sia $f(x) \in A[x]$. $\alpha \in A$ si dice* radice *o* zero *di $f(x)$ se $f(\alpha) = 0_A$ (i.e. la funzione polinomiale associata ad $f(x)$ valutata in α è pari a zero).*

Osservazione In $\mathbb{Z}/p\mathbb{Z}[x]$ il polinomio $x^p - x$ ha come radice ogni $\alpha \in \mathbb{Z}/p\mathbb{Z}$ in quanto ha funzione associata nulla.

Teorema 5.44 (Ruffini) *Sia K un campo. Sia $f(x) \in K[x]$.*
$\alpha \in K$ è radice di $f(x)$ se e solo se $(x-\alpha) \mid f(x)$.

***D**imostrazione.* Supponiamo $(x-\alpha) \mid f(x)$. Allora $f(x) = (x-\alpha)q(x)$ per qualche $q(x)$. Segue che $f(\alpha) = (\alpha-\alpha)q(x) = \underline{0}$. Viceversa supponiamo che $f(\alpha) = \underline{0}$. Dividiamo[1] $f(x)$ per $(x-\alpha)$:

$$f(x) = (x-\alpha)q(x) + r(x) \quad \text{con} \quad \text{gr}(r(x)) < \text{gr}(x-\alpha) = 1$$

Quindi $r(x)$ è una costante o è il polinomio nullo[2]. Ovvero $f(x) = (x-\alpha)q(x) + r$ con $r \in K$. Allora si ha:

$$\underline{0} = f(\alpha) = (\alpha-\alpha)q(\alpha) + r = r$$

E quindi $(x-\alpha) \mid f(x)$. ∎

Osservazioni

1. Un polinomio di grado 1 in $K[x]$ è irriducibile e ha una ed una sola radice in K. Infatti se $f(x) = a_1x + a_0$ con $a_1 \neq 0$ allora l'unico modo di fattorizzare $f(x)$ è come $h^{-1}(hf(x))$ con $h \neq 0$. L'unica radice di $f(x)$ è $\alpha := -a_1^{-1}a_0$. Quindi per il teorema di Ruffini se un polinomio di grado maggiore di 1 è irriducibile (in K) allora non ha radici (in K). Il viceversa non è vero. Ad esempio il polinomio $x^4 + 3x^2 + 2 = (x^2+1)(x^2+2) \in \mathbb{R}[x]$ non ha radici in $\mathbb{R}$ ma non è irriducibile.
2. Se $f(x) \in K[x]$ ha grado 2 oppure 3 allora è riducibile in $K[x]$ se e solo se ha radici in $K[x]$ (in ogni caso si trova un fattore di grado 1).

Definizione 5.33 *Sia K un campo e $f(x) \in K[x]$. Diremo che $\alpha \in K$ è radice di $f(x)$ di* molteplicità *$r \geq 1$ se $(x-\alpha)^r \mid f(x)$ ma $(x-\alpha)^{r+1} \nmid f(x)$.*

Esempi

1. Se $K = \mathbb{Z}/p\mathbb{Z}$ allora $x^p - x \in \mathbb{Z}/p\mathbb{Z}[x]$ ha funzione associata identicamente nulla. Segue che per il teorema di Ruffini:

   $$x^p - x = \prod_{\alpha \in \mathbb{Z}/p\mathbb{Z}} (x-\alpha)$$

   Quindi ogni $\alpha \in \mathbb{Z}/p\mathbb{Z}$ è radice *semplice* (di molteplicità 1).
2. In $\mathbb{Q}[x]$ il polinomio $x^4 - 2x^2 + 1 = (x+1)^2(x-1)^2$ come radici 1 e -1 ed entrambe hanno molteplicità 2. A garanzia di questo fatto è l'unicità di scrittura: a meno di costanti non nulle quello mostrato sopra è l'unico modo di fattorizzare il polinomio.
3. In $\mathbb{Z}/2\mathbb{Z}[x]$ il polinomio $x^4 - 2x^2 + 1 = (x+1)^4 = x^4 + 1$ ha 1 come radice di molteplicità 4.
4. Con un polinomio a coefficienti in un campo finito le radici si possono trovare semplicemente valutando il polinomio sui singoli elementi del campo e verificandone il risultato.

[1] Se K è in campo allora l'anello $K[x]$ è un dominio euclideo rispetto alla norma data dal grado di un polinomio.

[2] Le possibilità per il grado sono 0 oppure -1. Sel grado è 0 allora $r(x) = r$ è una costante (non nulla!). Se il grado è -1 allora $r(x) = 0$ è il polinomio nullo.

Teorema 5.45 *Sia K un campo e sia $0 \neq f(x) \in K[x]$ un polinomio di grado n. Allora la somma delle molteplicità delle radici di $f(x)$ in K non supera il grado n.*

***D**imostrazione.* Se $\mathrm{gr}(f(x)) = 0$ allora $f(x)$ non ha radici. Se $n > 0$ allora $f(x)$ è prodotto di fattori irriducibili (UFD) in $K[x]$. Se nessuno di questi fattori ha grado 1 allora $f(x)$ non ha radici. Altrimenti la decomposizione di $f(x)$ sarà della forma:

$$f(x) = k(x - \alpha_1)^{r_1} \dots (x - \alpha_s)^{r_s} g_1(x) \dots g_t(x)$$

Con $k \in K^*$, $\alpha_1, \dots, \alpha_s$ elementi distinti di K e i polinomi $g_i(x)$ sono irriducibili di grado maggiore di 1. Per l'unicità di fattorizzazione α_i é radice di molteplicità r_i per ogni $i = 1, \dots, s$. Inoltre $f(x)$ non ha altre radici [3] in K. D'altronde $r_1 + \dots + r_s \leq n$ e vale l'uguaglianza soltanto quando nella fattorizzazione di $f(x)$ non compare nessun irriducibile $g_i(x)$ di grado maggiore di 1. ∎

Osservazioni

1. Questo fatto vale in qualsiasi dominio di integrità. Infatti ogni dominio ha il suo campo delle frazioni. Se l'enunciato non valesse allora falsificherebbe l'enunciato anche nel caso dei campi (se $a \in \mathbb{Z}$ è radice di $f(x) \in \mathbb{Z}[x]$ allora $a/1 \in \mathbb{Q}$ è radice di $f(x) \in \mathbb{Q}[x]$).
2. L'enunciato del teorema è falso se A non è un dominio. Ad esempio in $\mathbb{Z}/6\mathbb{Z}[x]$ il polinomio $f(x) = x^2 - 5x$ ha come radici $0, 2, 3, 5$.

Corollario 5.46 *Se K è un campo* infinito *allora l'omomorfismo $\Phi : K[x] \to K^K$ che associa ad ogni polinomio la sua funzione polinomiale è iniettivo.*

***D**imostrazione.* Sia $f(x) \in \ker \Phi$. Alora la funzione polinomiale $F(x)$ è identicamente nulla, ovvero ogni elemento di K è radice. Ma se K è infinito per la proposizione precedente $f(x)$ non può che essere il polinomio nullo. ∎

Corollario 5.47 (Principio di identità dei polinomi)
Siano $\alpha_0, \alpha_1, \dots, \alpha_n$ $n+1$ elementi distinti di K. Se $a(x), b(x) \in K[x]$ sono due polinomi di grado $\leq n$ tali che $\forall\, i = 0, \dots, n$ $a(\alpha_i) = b(\alpha_i)$ allora $a(x) = b(x)$.

***D**imostrazione.* Sia $f(x) := a(x) - b(x)$. Allora $\mathrm{gr}(f(x)) \leq n$ e $f(\alpha_i) = a(\alpha_i) - b(\alpha_i) = 0$ per ogni $i = 0, \dots, n$. Quindi $f(x)$ ha $n+1$ radici distinte in K. Quindi contraddice il teorema 5.45 a meno che non sia il polinomio nullo. Ma allora $a(x) = b(x)$. ∎

Corollario 5.48 (Interpolatore di Lagrange)
Siano $\alpha_0, \alpha_1, \dots, \alpha_n$ $n+1$ elementi distinti di K. Se $\beta_0, \dots, \beta_n$ sono $n+1$ elementi (non necessariamente distinti) di K allora

$$\exists\, l(x) \in K[x] \;\; \textit{tale che} \;\; \forall\, i = 0, \dots, n \;\; l(\alpha_i) = \beta_i$$

***D**imostrazione.* L'unicità è una conseguenza immediata della proposizione precedente. Per l'esistenza poniamo

$$l(x) := \sum_{r=0}^{n} \left(\beta_r \prod_{j \neq r} \frac{x - \alpha_j}{\alpha_r - \alpha_j} \right)$$

Il polinomio $l(x)$ soddisfa le condizioni richieste. ∎

[3] Se $\beta \neq \alpha_i$ fosse un altra radice allora non potendo essere radice dei g_i ed essendo $(\beta - \alpha_i)^{r_i} \neq 0$ non potrebbe essere radice, assurdo.

Indice analitico