ALGEBRA: ANELLI, GRUPPI E CONGRUENZE

1. Prime proprietà dei gruppi

1.1. **La nozione di gruppo.** Iniziamo dalla definizione di gruppo:

Definizione 1.1. Un insieme G, dotato di un'operazione $\circ : G \times G \to G$ si dice *gruppo* se

- l'operazione $\circ$ è associativa;
- esiste in G un elemento e, detto "*identità*", tale che $e \circ x = x \circ e = x$ per ogni $x \in G$;
- ogni elemento $g \in G$ ammette un "*inverso*" $g^{-1} \in G$, tale cioè che $g \circ g^{-1} = g^{-1} \circ g = e$.

Scriverò spesso ab oppure $a \circ b$ invece del più pedante $\circ(a, b)$. Inoltre eviterò quasi sempre di scrivere parentesi per indicare l'ordine nel quale effettuare i prodotti. Questo è in effetti reso superfluo dall'associatività dell'operazione di gruppo. Richiedere che $(ab)c$ sia uguale ad $a(bc)$ basta ad assicurare che ogni possibile moltiplicazione di un numero qualsiasi di elementi dia lo stesso risultato, indipendentemente dall'ordine nel quale viene effettuato, a patto che si rispetti la posizione di ciascun fattore. Ad esempio, per il prodotto di quattro elementi, l'associatività comporta che:

$$a(b(cd)) = a((bc)d) = (a(bc))d = ((ab)c)d = (ab)(cd),$$

il che mostra che trascurare le parentesi e scrivere $abcd$ non è solo un abuso di notazione, ma la conseguenza di un fenomeno naturale. Di questo bisognerebbe dare una dimostrazione rigorosa. Farlo è semplice, ma letta la dimostrazione le idee potrebbero essere più confuse di prima.[1]

Una notazione compatta per i prodotti $aa, aaa, \dots$ consiste nello scrivere, come già si fa per il prodotto di numeri, $a^2, a^3, \dots$ Con a^{-n} indicherò $(a^{-1})^n$, che coincide con $(a^n)^{-1}$. E' facile convincersi che $a^m a^n = a^{m+n}$ e che $(a^m)^n = a^{mn}$, se si pone $a^0 = e, a^1 = a$.

L'associatività è una richiesta scontata quando gli elementi del nostro gruppo siano permutazioni su di un insieme, e come la stragrande maggioranza degli esempi di gruppi possano essere interpretati come azioni geometriche su di insiemi particolari, come ad esempio rotazioni in un piano, traslazioni su una retta, ecc... In tutti questi casi, l'operazione è la composizione di applicazioni, che è naturalmente associativa.

Esempi:

- L'insieme S_X di tutte le applicazioni invertibili da un insieme X in se stesso, con l'operazione di composizione, è un gruppo, detto il *gruppo delle permutazioni di* X. Se X è un insieme finito, allora si sceglie solitamente $X = \{1, 2, ..., n\}$ e si scrive $\mathrm{S}_X = \mathrm{S}_n$. Il gruppo simmetrico S_n ha $n!$ elementi.
- L'insieme delle rotazioni nel nel piano centrate nell'origine di angoli multipli di $2\pi/n$ è un gruppo, che si indica con C_n. Abbiamo visto che questo gruppo possiede n elementi, e che è un gruppo *ciclico*. Esso ammette cioè un elemento le cui potenze esauriscano tutti gli elementi del gruppo. Un elemento di tale tipo è detto *generatore* del gruppo ciclico. Ad esempio, la rotazione di $2\pi/n$ genera il gruppo ciclico C_n.
- L'insieme $\mathrm{GL}_n(\mathbb{K})$ delle matrici $n \times n$ **non singolari**, cioè di determinante non nullo, a coefficienti in un campo $\mathbb{K}$ (ad esempio il campo $\mathbb{K} = \mathbb{R}$ dei numeri reali) è un gruppo rispetto al prodotto righe per colonne. Tale prodotto è infatti associativo, ed il prodotto di matrici di determinante non nullo è ancora una matrice di determinante non nullo. Inoltre l'identità ha determinante $1 \neq 0$, ed ogni matrice non singolare ha per inversa una matrice ancora non singolare.
- L'insieme $\mathrm{SL}_n(\mathbb{K})$ delle matrici n per n di determinante 1 è ancora un gruppo, sempre rispetto al prodotto righe per colonne.
- Gli insiemi numerici $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, se considerati con l'operazione $+$ di **somma**, sono gruppi. L'identità è in tutti i casi l'elemento 0, mentre l'inverso di α è $-\alpha$.

La notazione additiva nell'ultimo esempio non deve fuorviare: $+$ è decisamente un'operazione di gruppo. Indicare l'operazione di gruppo con $+$ invece che $\cdot$ è estremamente frequente quando l'operazione è commutativa, cioè quando $ab = ba$ per ogni coppia di elementi $a, b \in G$. Questi gruppi sono detti *abeliani*. Chiaramente, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sono abeliani. E' abeliano anche C_n, mentre non lo sono S_X, GL_n ed S_n.[2] Ora alcuni

Non-esempi:

- La famiglia E_X di tutte le applicazioni dall'insieme X in se stesso non è un gruppo.[3] In effetti, la composizione è un'operazione associativa, e l'identità ne è l'elemento neutro. Però un'applicazione ha inversi sinistri se e solo se è iniettiva, ed ha inversi destri se e solo se è suriettiva. Quindi non tutti gli elementi di E_X ammettono inverso.
- L'insieme delle matrici $n \times n$ di determinante nullo non è un gruppo, rispetto al prodotto righe per colonne. Pur essendo tale prodotto associativo, e il prodotto di matrici singolari ancora singolare, non esiste in questo caso un elemento neutro per il prodotto.
- Gli insiemi di matrici $\mathrm{GL}_n(\mathbb{K}), \mathrm{SL}_N(\mathbb{K})$ non sono gruppi rispetto all'operazione di somma tra matrici.
- Gli insiemi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ non sono gruppi se considerati con l'operazione di moltiplicazione. Infatti l'elemento 0 non ammette un inverso moltiplicativo. $\mathbb{Q} \setminus \{0\}$ e $\mathbb{R} \setminus \{0\}$ sono tuttavia gruppi rispetto alla moltiplicazione; più in generale, se A è un anello, l'insieme $A^\times$ degli elementi (moltiplicativamente) invertibili di A è un gruppo rispetto alla moltiplicazione.

A lezione, abbiamo visto che

Teorema 1.2. *In un gruppo G esiste un'unica identità. Ogni elemento ammette un solo inverso. Inoltre $(g^{-1})^{-1} = g$, $(gh)^{-1} = h^{-1}g^{-1}$.*

[1] Ogni volta che si cerca di dimostrare un fatto intuitivo ed ovvio, si scopre che la dimostrazione non chiarisce nulla, oppure che il fatto era falso.

[2] A dire il vero, S_X è abeliano se X contiene meno di tre elementi, mentre GL_n ed SL_n sono abeliani se $n \leq 1$.

[3] ...a meno che X abbia meno di due elementi.

Dimostrazione. Siano e, e' elementi neutri per l'operazione di gruppo. Questo vuol dire che

$$ex = xe = e, \qquad e'x = xe' = x$$

per ogni scelta di $x \in G$. In particolare $e = ee' = e'$, e quindi vi è un solo elemento neutro.

Si procede in maniera analoga per mostrare l'unicità dell'inverso: se x e y sono entrambi inversi di g, allora $gx = xg = e$, $gy = yg = e$. Ne segue che $x = xe = xgy = ey = y$, e quindi vi è un solo inverso di g. Le altre due proprietà seguono subito osservando che $gg^{-1} = g^{-1}g = e$, $ghh^{-1}g^{-1} = geg^{-1} = e$. □

Si vede che per invertire il prodotto gh bisogna moltiplicare gli inversi degli elementi g e h, **ma nell'ordine inverso**. Questo dipende dalla (possibile) non commutatività del prodotto. In un gruppo abeliano si avrebbe chiaramente $(ab)^{-1} = a^{-1}b^{-1}$. La stessa avvertenza è da fare con le potenze di un prodotto: infatti $(ab)^3$ non è l'elemento a^3b^3, bensì $ababab$!!!

1.2. **Omomorfismi di gruppi.** Siano G, H due gruppi.

Definizione 1.3. $\phi : G \to H$ è un *omomorfismo di gruppi*, o più semplicemente un *omomorfismo*, se

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

per ogni scelta di $a, b \in G$. Un omomorfismo invertibile si dice *isomorfismo*, mentre un isomorfismo di un gruppo su se stesso si dice *automorfismo*.

Proposizione 1.4. *Se $\phi : G \to H$ è un omomorfismo di gruppi, allora*

- $\phi(e) = e$;
- $\phi(g^{-1}) = \phi(g)^{-1}$ *per ogni* $g \in G$.

Dimostrazione. Poiché $e \cdot e = e$ in G, si ha $\phi(e) = \phi(e \cdot e) = \phi(e) \cdot \phi(e)$. Moltiplicando a sinistra per l'inverso di $\phi(e)$ in H si ottiene $\phi(e) = e$. Allo stesso modo, da $g \cdot g^{-1} = e$ segue $e = \phi(e) = \phi(g \cdot g^{-1}) = \phi(g)\phi(g^{-1})$. Di conseguenza, $\phi(g^{-1})$ è l'inverso di $\phi(g)$. □

Esempi:

- L'applicazione che manda ogni elemento del gruppo G nell'identità di un altro gruppo è un omomorfismo.
- L'applicazione identità da un gruppo in sé è un omomorfismo. E' l'automorfismo identico del gruppo
- L'applicazione $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\}$ è un omomorfismo. Infatti $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$ per ogni $\sigma, \tau \in \mathrm{S}_n$.
- L'applicazione $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ che manda ogni matrice M nel suo determinante $\det M \in \mathbb{K}^* = \mathbb{K} \setminus \{0\}$ è un omomorfismo. Infatti $\det(AB) = \det(A)\det(B)$.
- L'applicazione $\exp : (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$ definita come $\exp(x) = e^x$ è un omomorfismo di gruppi. Infatti l'operazione di gruppo di $\mathbb{R}$ è la somma, e si ha $\exp(x + y) = \exp(x)\exp(y)$.
- Se g è un elemento del gruppo G, $n \mapsto g^n$ definisce un omomorfismo $(\mathbb{Z}, +) \to G$. Infatti $g^m g^n = g^{m+n}$.
- Ogni spazio vettoriale può essere visto come gruppo abeliano rispetto alla sola operazione di somma tra vettori. Allora un'applicazione lineare tra spazi vettoriali è sempre un omomorfismo di gruppi.

Sia $\phi : G \to H$ un omomorfismo.

Definizione 1.5. Il *nucleo* di ϕ è l'insieme degli elementi g di G tali che $\phi(g) = e$. L'*immagine* di ϕ è l'insieme degli elementi $h \in H$ per i quali esiste $g \in G$ tale che $\phi(g) = h$.

Indicheremo il nucleo e l'immagine di un omomorfismo ϕ con $\ker \phi$, $\mathrm{Im}\phi$ rispettivamente.

Esempi:

- L'applicazione identità da un gruppo in sé è un omomorfismo iniettivo; infatti solo l'elemento neutro giace nel suo nucleo. L'immagine coincide con l'intero gruppo.
- Il nucleo di $\mathrm{sgn} : \mathrm{S}_n \to \{\pm 1\}$ è il sottoinsieme A_n delle permutazioni pari.
- Se $\mathbb{K}$ è un campo, il nucleo di $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ è dato dal sottoinsieme $\mathrm{SL}_n(\mathbb{K})$ delle matrici di determinante 1. L'immagine è tutto $\mathbb{K}^*$.
- L'omomorfismo $\exp : \mathbb{R} \to \mathbb{R}^*$ non è un isomorfismo. E' infatti iniettivo, poiché $e^x = 1 \Rightarrow x = 0$, ma non è suriettivo, poiché la sua immagine contiene i soli numeri reali positivi.
- L'omomorfismo $\mathbb{Z} \ni n \mapsto g^n \in G$ ha per immagine il sottoinsieme di G i cui elementi sono tutte e sole le potenze di g. Descriveremo il nucleo di questo omomorfismo più tardi.
- Se $n \neq 0, 1$, l'applicazione $G \ni g \mapsto g^n \in G$ non è in generale un omomorfismo. Ad ogni modo, quando G è un gruppo abeliano, allora è un omomorfismo per ogni n.

1.3. **Sottogruppi.**

Definizione 1.6. Sia G un gruppo. Un sottoinsieme non vuoto $H \subset G$ si dice *sottogruppo*, se H ammette una struttura di gruppo **rispetto allo stesso prodotto** di G.

Per indicare che H è un sottogruppo di G, si usa la notazione $H < G$. Si vede facilmente che, se $H < G$, allora le identità di H e di G coincidono, e l'inverso di un elemento in H è lo stesso che in G. Dal momento che l'operazione di gruppo di G ristretta ad H è automaticamente associativa, abbiamo

Proposizione 1.7. *Affinché un sottoinsieme $H \subset G$ sia un sottogruppo di G è sufficiente*[4] *che:*

- $e \in H$;
- *se* $a, b \in H$ *allora anche* $ab \in H$;
- *se* $a \in H$ *allora anche* $a^{-1} \in H$.

Dimostrazione. Poiché il prodotto di elementi di H rimane dentro H, la restrizione del prodotto di G ad elementi di H definisce un'operazione $H \times H \to H$, che è automaticamente associativa. L'identità e di G è allora un elemento neutro di H, e ogni elemento di H ha un inverso in H perché è stato esplicitamente imposto. □

[4] Nonché ovviamente necessario!

La verifica che $e \in H$ può essere evitata se è noto che H sia un sottoinsieme non vuoto: in effetti, se $h \in H$, allora anche $h^{-1} \in H$, e quindi $hh^{-1} = e \in H$. Tuttavia, in tutte le situazioni concrete, la maniera più semplice di verificare che un sottogruppo di G sia non vuoto è quella di controllare che contenga l'identità di G.

Esempi:

- I sottoinsiemi $\{e\}$ e G sono sempre sottogruppi di G: sono detti *sottogruppi banali*.
- Comunque sia scelto $m \in \mathbb{Z}$, l'insieme di tutti i multipli di m è un sottogruppo di $\mathbb{Z}$.
- SL_n è un sottogruppo di GL_n.
- Sia $g \in G$. L'insieme di tutte le potenze positive e negative $\langle g \rangle = \{g^i | i \in \mathbb{Z}\}$ è un sottogruppo di G. Il sottogruppo $\langle g \rangle$ è sempre abeliano.

Proposizione 1.8. *Se $\phi : G \to H$ è un omomorfismo di gruppi, allora* $\ker \phi < G$ *e Im* $\phi < H$.

Dimostrazione. Mostriamo innanzitutto che $\ker \phi$ è un sottogruppo di G: abbiamo già visto che $\phi(e) = e$, e quindi $e \in \ker \phi$.

Se $a, b \in \ker \phi$, allora $\phi(a) = \phi(b) = e$ e quindi $\phi(ab) = \phi(a)\phi(b) = e \cdot e = e$. Analogamente, se $a \in \ker \phi$, allora $\phi(a^{-1}) = \phi(a)^{-1} = e^{-1} = e$. Pertanto $\ker \phi$ contiene l'identità, ed è chiuso rispetto a prodotto e inverso.

Il fatto che l'immagine sia un sottogruppo di H è anche più semplice. L'identità appartiene all'immagine in quanto $\phi(e) = e$. Da $\phi(ab) = \phi(a)\phi(b)$, $\phi(a^{-1}) = \phi(a)^{-1}$ segue che il prodotto e l'inverso di elementi di Im ϕ appartengono ancora ad Im ϕ. □

1.4. **Intersezione e prodotto di sottogruppi.** Studiando l'algebra lineare, abbiamo già visto che l'intersezione di sottospazi vettoriali è un sottospazio vettoriale. Per ottenere il sottospazio generato da due sottospazi vettoriali non era invece sufficiente prendere l'unione dei due sottospazi, ma piuttosto la *somma* dei due, ovvero l'insieme di tutte le somme di un elemento del primo sottospazio con un elemento del secondo.

La situazione, nel caso dei gruppi abeliani, è praticamente la stessa. Per quanto riguarda quelli non abeliani bisogna prestare, invece, qualche attenzione.

Proposizione 1.9. *L'intersezione $H \cap K$ di due sottogruppi $H, K < G$ è un sottogruppo di G.*

Dimostrazione. $H \cap K$ è non vuoto, dal momento che l'identità e vi appartiene sicuramente. Per mostrare che se $a, b \in H \cap K$ allora $ab \in H \cap K$ basta notare che a e b appartengono entrambi sia ad H che a K. Essendo questi insiemi sottogruppi, sono chiusi rispetto al prodotto, perciò ab giace sia in H che in K, quindi nella loro intersezione. Per quanto riguarda l'inverso, il ragionamento è del tutto analogo. □

Proposizione 1.10. *Il prodotto $HK = \{hk | h \in H, k \in K\}$ di sottogruppi di G è un sottogruppo se e solo se $HK = KH$.*

Dimostrazione. Siano h, k elementi di H, K rispettivamente. Allora $h^{-1} \in H, k^{-1} \in K$ e quindi $h^{-1}k^{-1} \in HK$. Se HK è un sottogruppo, allora deve contenere anche l'inverso di $h^{-1}k^{-1}$; ma $(h^{-1}k^{-1})^{-1} = kh$ e quindi $kh \in HK$. Al variare di $h \in H$, $k \in K$ si ottiene $KH \subset HK$.

In modo simile, poiché $k^{-1}h^{-1} \in KH \subset HK$, allora è possibile trovare $h' \in H, k' \in K$ tali che $k^{-1}h^{-1} = h'k'$. Prendendo l'inverso di entrambi i membri, si ottiene $hk = (k')^{-1}(h')^{-1} \in KH$, e quindi si ha anche l'altra inclusione $HK \subset KH$. □

Proposizione 1.11. *Il sottoinsieme HK ha esattamente $|H||K|/|H \cap K|$ elementi.*

Dimostrazione. Consideriamo l'applicazione $\mu : H \times K \ni (h, k) \mapsto hk \in G$. Si vede subito che $\mu(h_1, k_1) = \mu(h_1 d^{-1}, dk_1)$ per ogni scelta di $d \in H \cap K$.

Viceversa, se $\mu(h_1, k_1) = \mu(h_2, k_2)$, allora $h_1 k_1 = h_2 k_2$, cioè $h_2^{-1} h_1 = k_2 k_1^{-1}$; se indichiamo tale elemento con d, sicuramente $d \in H \cap K$, $h_2 = h_1 d^{-1}$, $k_2 = dk_1$. Questo mostra che ogni elemento nell'immagine HK di μ è raggiunto da esattamente $|H \cap K|$ elementi di $H \times K$: pertanto $|H||K| = |H \times K| = |HK||H \cap K|$. □

Corollario 1.12. *Se G è abeliano, e $H, K < G$, allora HK è sempre un sottogruppo.*

Nel caso si stia utilizzando la notazione additiva all'interno di un gruppo, si scriverà ovviamente $H + K$ invece di HK.

Esempio: Sia $\mathbb{F}_p = \mathbb{Z}/(p)$ il campo delle classi di resto modulo p, dove p è un numero primo. Uno spazio vettoriale U di dimensione n sul campo $\mathbb{F}_p$ è isomorfo a $\mathbb{F}_p^n$ e contiene pertanto p^n elementi. Ogni sottospazio vettoriale di U è in particolare un sottogruppo del gruppo additivo $(U, +)$. Se $V, W \subset U$ sono sottospazi vettoriali, e quindi sottogruppi additivi, si ottiene $|V + W| = |V||W|/|V \cap W|$, da cui

$$p^{\dim(V+W)} = p^{\dim V} p^{\dim W} / p^{\dim(V \cap W)},$$

e quindi $p^{\dim(V+W)+\dim(V\cap W)} = p^{\dim V + \dim W}$. Si nota immediatamente l'analogia con la formula di Grassmann $\dim(V + W) + \dim(V \cap W) = \dim V + \dim W$ che vale per sottospazi vettoriali (di dimensioni finita) di uno spazio vettoriale qualsiasi.

Vediamo ora una generalizzazione del sottogruppo $\langle g \rangle$ generato da un elemento.

Definizione 1.13. Sia G un gruppo, e $X \subset G$ un suo sottoinsieme. Il *sottogruppo di G generato da X* è l'intersezione

$$\langle X \rangle = \bigcap_{H < G, X \subset H} H$$

dei sottogruppi di G che contengono X.

L'intersezione di una collezione di sottogruppi di G è ancora un sottogruppo — la dimostrazione data precedentemente nel caso di due soli sottogruppi si generalizza facilmente — e quindi $\langle X \rangle$ è sicuramente un sottogruppo di G, e contiene chiaramente X. Per come è stato definito, è il *più piccolo sottogruppo di G che contenga X*, il che giustifica il nome di sottogruppo generato da X.

Se $H, K < G$, si preferisce indicare $\langle H \cup K \rangle$ con $\langle H, K \rangle$; in modo analogo, si indica $\langle \{g_1, \ldots, g_r\} \rangle$ semplicemente con $\langle g_1, \ldots, g_r \rangle$. E' evidente che $\langle H, K \rangle$ contiene sia H che K, e quindi anche i prodotti HK, KH. Questo mostra che se HK è un sottogruppo di G, allora $\langle H, K \rangle = HK$, a causa della minimalità del sottogruppo generato.

2. Sottogruppi di $\mathbb{Z}$ e ordine di elementi

2.1. **Il gruppo $\mathbb{Z}$.** L'insieme $\mathbb{Z}$, con l'operazione $+$ di somma, costituisce un gruppo abeliano. Infatti, $+$ è un'operazione commutativa ed associativa, della quale 0 è l'elemento neutro. Inoltre, $-n$ è un inverso (additivo) dell'elemento n, e pertanto ogni elemento ammette inverso. $\mathbb{Z}$ è un gruppo ciclico; i suoi due generatori ciclici sono 1 e -1. Nel caso del gruppo $\mathbb{Z}$, è tradizione indicare il sottogruppo generato da un sottoinsieme X con (X) invece che con $\langle X\rangle$. Il sottoinsieme $(n) \subset \mathbb{Z}$, composto dai multipli di un intero n fissato, è un sottogruppo (ancora ciclico) di $\mathbb{Z}$.

Teorema 2.1. *I sottogruppi di $\mathbb{Z}$ sono tutti della forma (n), per qualche $n \in \mathbb{N}$.*

Dimostrazione. Sia H un sottogruppo di $\mathbb{Z}$. Se contiene solo lo 0, allora $H = (0)$ ed abbiamo concluso. Se invece H non contiene solo lo (0), contiene allora certamente elementi positivi. Sia n il minimo elemento positivo di H.

Allora $H = (n)$. Infatti, H contiene certamente tutti i multipli di n. Inoltre, H non può contenere un elemento a non multiplo di n. Dovrebbe infatti contenere anche il resto della divisione di a per n: in effetti, se $a = qn + r$, allora il resto $r = a + (-q) \cdot n$ appartiene ad H poiché sia a che $(-q)n$ appartengono ad H. Se il resto r è diverso da 0, è allora un elemento positivo di H minore di n, da cui un assurdo. □

Proposizione 2.2. *Siano c e d il minimo comune multiplo ed il massimo comun divisore degli interi a ed b. Allora $(a)\cap(b) = (c), (a)+(b) = (d)$.*

Dimostrazione. $(a)\cap(b)$ è sicuramente un sottogruppo, i cui elementi sono multipli sia di a che di b. Il suo minimo elemento positivo è pertanto c, da cui $(a) \cap (b) = (c)$. Anche $(a) + (b)$ è un sottogruppo, pertanto della forma (d). Gli interi a e b appartengono a (d), pertanto d è un divisore comune di a e b.

Per mostrare che d è il massimo tra i divisori comuni di a e b, notiamo dapprima che $d \in (a) + (b)$, e che quindi si può scrivere come somma di un multiplo di a e di uno di b. In altre parole esistono interi m, n tali che $d = ma + nb$. Se d' è un divisore comune di a e b, allora deve dividere anche $d = ma + nb$, e pertanto $d' \leq d$. In altre parole, d è il più grande tra i divisori comuni di a e b. □

2.2. **Ordine di elementi.**

Definizione 2.3. Sia G un gruppo. Si dice che $g \in G$ ha *ordine infinito* se nessuna potenza di g di esponente positivo è uguale all'identità. Altrimenti, l'*ordine* di g è il minimo intero positivo n tale che $g^n = e$.

Ad esempio, l'identità ha sempre ordine 1, mentre ogni elemento non nullo di $(\mathbb{Z}, +)$ ha ordine infinito. L'ordine di g si indica con $o(g)$. L'ordine di un elemento $g \in G$ può essere meglio compreso attraverso l'omomorfismo $\phi : \mathbb{Z} \to G$ definito da $\phi(n) = g^n$. Si vede subito che ϕ è un omomorfismo di gruppi: per verificare $\phi(m+n) = \phi(m)\phi(n)$ è sufficiente controllare che $g^m g^n = g^{m+n}$, cosa che abbiamo già fatto.

L'immagine di ϕ è il sottoinsieme di G formato da tutte e sole le potenze di g. E' sicuramente un sottogruppo, in quanto immagine di un omomorfismo. Il nucleo di ϕ è un sottogruppo di $\mathbb{Z}$, ed è quindi della forma (d), dove $d \geq 0$. Quando $d = 0$, il nucleo di ϕ è banale, e ϕ è pertanto iniettiva; in questo caso tutte le potenze di g sono distinte e il sottogruppo (g) contiene infiniti elementi.

Quando $\ker \phi = (d)$, d è certamente il più piccolo esponente positivo tale che $g^d = e$, ed è quindi l'ordine di g. L'immagine è nuovamente un sottogruppo, ma molte potenze di g coincidono tra loro. In effetti, le uniche potenze distinte di g sono $1, g, g^2, \ldots, g^{d-1}$ e di conseguenza il sottogruppo generato da g contiene esattamente d elementi. In conclusione, l'ordine di g coincide con il numero di elementi nel sottogruppo generato da g.

Teorema 2.4. *Ogni elemento di un gruppo finito ha ordine finito.*

Dimostrazione. A questo punto l'affermazione è evidente: se g è un elemento di un gruppo finito G, il sottogruppo $(g) \subset G$ deve possedere un numero finito di elementi, e pertanto g ha ordine finito. □

Teorema 2.5. *Un gruppo di ordine pari possiede almeno un elemento di ordine 2.*

Dimostrazione. Creiamo una partizione del gruppo G in sottoinsiemi del tipo $\{g^{\pm 1}\}$. Poiché $(g^{-1})^{-1} = g$, i sottoinsiemi sono disgiunti o coincidono. Ciascun sottoinsieme contiene due elementi, oppure uno nel caso in cui $g^{-1} = g$; questo accade esattamente quando $g^2 = 1$, cioè quando g ha ordine 1 oppure 2.

G risulta ripartito in alcuni sottoinsiemi di due elementi, che danno in totale un numero pari di elementi, e in alcuni sottoinsiemi di un elemento: tra questi vi è sicuramente l'identità, che è l'unico elemento di ordine 1.

Se non vi fossero elementi di ordine 2, G avrebbe complessivamente un numero dispari di elementi. Poiché l'ordine di G è pari, deve allora possedere almeno un elemento di ordine 2. □

Teorema 2.6. *Il numero di elementi di un campo finito di ordine pari è una potenza di 2.*

Dimostrazione. Se F è un campo, $(F, +)$ è un gruppo abeliano. Se F è un campo finito di ordine pari, allora $(F, +)$ possiede almeno un elemento di ordine 2: esiste cioè un elemento $x \neq 0$ tale che $x + x = 0$.

Moltiplicando per l'inverso moltiplicativo di x, si ottiene $1 + 1 = 0$, e quindi $K = \{0, 1\}$ è un sottocampo con esattamente 2 elementi. F è allora un K-spazio vettoriale, di dimensione n finita, a causa della finitezza di F — uno spazio vettoriale con un numero finito di elementi non può certamente avere una base infinita! Allora F è isomorfo a K^n come spazio vettoriale. In particolare, ha la stessa cardinalità di K^n, che possiede 2^n elementi. □

Teorema 2.7 (Cauchy)**.** *Se p è un numero primo e p divide $|G|$, allora esiste un elemento di G di ordine p.*

Dimostrazione. L'insieme $\Gamma = \{(g_1, g_2, \ldots, g_p) | g_1 g_2 \ldots g_p = 1\}$ possiede $|G|^{p-1}$ elementi. Se $(g_1, g_2, \ldots, g_p) \in \Gamma$, allora anche $(g_2, g_3, \ldots, g_p, g_1) \in \Gamma$.

Se gli elementi g_i non sono tutti uguali, ruotando ciclicamente $(g_1, g_2, \ldots, g_p)$ si ottengono p elementi distinti. Pertanto possiamo disporre gli elementi di Γ in parti di p elementi che si ottengono l'uno dall'altro per permutazioni ciclica, e in singoli elementi della forma $(g, g, \ldots, g)$. Poiché $|\Gamma|$ è multiplo di p, gli elementi di Γ della forma $(g, g, \ldots, g)$ sono anch'essi in numero multiplo di p. Poiché $(1, 1, \ldots, 1) \in \Gamma$, sono almeno p. Basta ora osservare che se $(g, g, \ldots, g) \in \Gamma$, allora $g^p = 1$, e quindi g ha ordine p non appena $g \neq 1$.

□

Teorema 2.8. *Il numero di elementi di un campo finito è sempre potenza di un primo.*

Dimostrazione. Sia p un numero primo che divide l'ordine del campo. Usare il Teorema di Cauchy e procedere come nel caso $p = 2$ già trattato sopra. □

2.3. **Congruenze modulo un sottogruppo e classi laterali.** Il concetto di congruenza modulo un sottogruppo generalizza quello di congruenza modulo n nel gruppo $\mathbb{Z}$ degli interi, e permette di mostrare il fondamentale teorema di Lagrange, che è punto di partenza per lo studio dei gruppi finiti. Siano G un gruppo, e H un suo sottogruppo.

Definizione 2.9. Se $a, b \in G$, si dice che a è *congruo* a b modulo H, e si scrive

$$a \equiv b \mod H$$

se $a^{-1}b \in H$.

Teorema 2.10. *La congruenza modulo H è una relazione di equivalenza.*

La dimostrazione è immediata. Qui è sufficiente ricordare che una relazione $\sim$ su di un insieme X si dice *relazione di equivalenza* se valgono:

- $a \sim a$ (proprietà riflessiva)
- Se $a \sim b$ allora anche $b \sim a$ (proprietà simmetrica)
- Se $a \sim b$ e $b \sim c$ allora anche $a \sim c$ (proprietà transitiva)

per ogni scelta di $a, b, c \in X$.

Una classe di equivalenza è un sottoinsieme di elementi tutti equivalenti tra loro. Le relazioni di equivalenza servono a ripartire un insieme in unione disgiunta di classi di equivalenza. Questo dipende dal fatto che, a causa della proprietà transitiva, classi di equivalenza che hanno intersezione non vuota sono uguali: hanno cioé esattamente gli stessi elementi. Due classi di equivalenza sono disgiunte, oppure coincidono!

Nel caso della relazione di congruenza modulo un sottogruppo H, le classi di equivalenza sono facili da determinare. Abbiamo infatti mostrato a lezione che gli elementi congrui ad $a \in G$ modulo H sono tutti e soli quegli elementi di G che si scrivono come ha per qualche elemento $h \in H$.

Proposizione 2.11. *La classe di congruenza modulo H dell'elemento $a \in G$ coincide con il sottoinsieme $aH = \{ah \mid h \in H\}$.*

Dimostrazione. $a \equiv b \mod H$ se e solo se $a^{-1}b \in H$. Ad ogni modo, $a^{-1}b = h \in H$ è equivalente a $b = ah \in aH$. In altre parole, gli elementi in relazione con a sono tutti e soli quelli che giacciono in aH. □

I sottoinsiemi del tipo aH si dicono *classi laterali sinistre*, o semplicemente *laterali sinistri*, di H in G. Avremmo potuto definire la relazione di congruenza modulo H anche tramite la condizione $ab^{-1} \in H$. Questa nuova condizione non è equivalente all'altra che abbiamo dato, e fornisce una relazione differente. Le sue classi di equivalenza sono date dai laterali destri Ha invece che da quelli sinistri. I sottogruppi per i quali i laterali sinistri coincidono con quelli destri, e quindi le due relazioni coincidono, si chiamano *sottogruppi normali*, e rivestono un ruolo rilevante nella teoria dei gruppi.

L'insieme dei laterali sinistri di H in G, cioè l'insieme quoziente per la relazione di congruenza sopra introdotta, si indica con G/H, mentre quello dei laterali destri possiede la strana notazione $H\backslash G$.

Proposizione 2.12. *Gli insiemi G/H e $H\backslash G$ hanno la stessa cardinalità.*

Dimostrazione. L'applicazione $g \mapsto g^{-1}$ si restringe ad una bigezione $xH \mapsto Hx^{-1}$. □

Come conseguenza, anche nel caso di gruppi infiniti, l'indice di un sottogruppo è un concetto ben definito, ed indipendente dalla decisione di considerare laterali destri o sinistri.

2.4. **Il Teorema di Lagrange e le sue conseguenze.** La proprietà rilevante dei laterali sinistri di un sottogruppo $H < G$ è che hanno tutti la stessa cardinalità.

Proposizione 2.13. *L'applicazione $H \ni h \mapsto ah \in aH$ è una corrispondenza biunivoca.*

Dimostrazione. La suriettività segue dalla stessa definizione di aH. L'iniettività è facile: se $ah_1 = ah_2$, allora moltiplicando a sinistra per a^{-1} si ottiene $h_1 = h_2$. □

Definizione 2.14. L'ordine di un gruppo G è il numero dei suoi elementi, e si indica con $|G|$.

Definizione 2.15. L'indice di un sottogruppo H, nel gruppo G che lo contiene, è il numero dei laterali sinistri di H in G (ovvero la cardinalità dell'insieme quoziente G/H), e si indica con $[G : H]$.

La conclusione è immediata. G è un insieme che viene ripartito in laterali sinistri aH che hanno tutti la stessa cardinalità di H. Se il numero di laterali destri è $[G : H]$ allora si ha:

Teorema 2.16. *Se $H < G$ sono gruppi finiti, allora $|G| = [G : H]|H|$*

La notazione utilizzata per l'indice di H in G è suggestiva, infatti $[G : H] = |G|/|H|$. Il "diviso"non è solo un segno di interpunzione: è davvero, in qualche senso, un'operazione di divisione!

Osservazione 2.17. L'identità $|G| = [G : H]|H|$ è effettivamente un'uguaglianza tra cardinalità. In effetti, una volta scelto[5] un elemento x_α per ogni laterale sinistro di H in G, l'applicazione

$$G/H \times H \ni (x_\alpha H, h) \mapsto x_\alpha h \in G$$

fornisce una corrispondenza biunivoca.

Teorema 2.18 (Lagrange)**.** *Se H è un sottogruppo del gruppo finito G, allora l'ordine di H divide quello di G.*

Corollario 2.19. *Se g è un elemento del gruppo finito G, allora l'ordine di g divide quello di G. In particolare $g^{|G|} = e$.*

[5]Questo richiede tuttavia l'utilizzo dell'assioma della scelta.

Dimostrazione. L'ordine dell'elemento g è pari a quello del sottogruppo

$$\langle g\rangle = \{e, g, g^2, \dots, g^{n-1}\}$$

generato da g. Inoltre, $|G| = o(g)\cdot[G:(g)]$, quindi

$$g^{|G|} = g^{o(g)\cdot[G:(g)]} = (g^{o(g)})^{[G:(g)]} = e^{[G:(g)]} = e.$$

□

Corollario 2.20. *Un gruppo di ordine primo è ciclico, e i suoi unici sottogruppi sono quelli banali.*

Dimostrazione. Sia $|G| = p$, con p primo. L'ordine degli elementi di G divide p, e può quindi essere uguale solo ad 1 oppure a p. L'identità è l'unico elemento che ha ordine 1, e tutti gli altri devono avere ordine p. Questo vuol dire che per ogni scelta di $e \neq g \in G$, il sottogruppo $\langle g\rangle$ possiede p elementi, e coincide quindi con H. In conclusione, G è ciclico.

I sottogruppi sono necessariamente banali per lo stesso motivo: l'ordine di un sottogruppo è 1 oppure p, e pertanto ogni dato sottogruppo contiene solo l'identità, oppure tutti gli elementi del gruppo G. □

2.5. **Sottogruppi normali.** In un gruppo abeliano G, ciascun laterale sinistro di un sottogruppo $H < G$ è anche un laterale destro. In effetti, dal momento che l'operazione è commutativa, si ha necessariamente $aH = Ha$.

Questo non è sempre vero, come si verifica facilmente nel seguente esempio:

Esempio 2.21. Sia $G = \mathrm{S}_3$, $H = \langle(1\,2)\rangle$. Allora $(1\,3)H = \{(1\,3), (1\,2\,3)\}$, mentre $H(1\,3) = \{(1\,3), (1\,3\,2)\}$.

Si vede subito che, se $aH = Ha$, moltiplicando per a^{-1} a destra si ottiene $aHa^{-1} = H$. Istituzionalizziamo questo fatto ad una definizione

Definizione 2.22. Un sottogruppo $H < G$ è normale se $ghg^{-1} \in H$ ogni volta che $h \in H, g \in G$.

Quando H è un sottogruppo normale di G, si scrive $H \lhd G$.

Proposizione 2.23. *Se $\phi : G \to H$ è un omomorfismo di gruppi, allora* $\ker\phi \lhd G$.

Dimostrazione. Se $h \in \ker\phi$, allora $\phi(h) = e$. Di conseguenza $\phi(ghg^{-1}) = \phi(g)e\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = e$, quindi $ghg^{-1} \in \ker\phi$. □

L'importanza dei sottogruppi normali giace nel fatto che l'operazione di G induce un'operazione ben definita sull'insieme dei laterali sinistri di un sottogruppo H se e solo se $H \lhd G$. Vediamo perché:

Teorema 2.24. *Sia $H < G$ e utilizziamo la notazione $[a] = aH$. Allora l'operazione $[a][b] = [ab]$ è ben definita se e solo se $H \lhd G$.*

Dire che l'operazione è ben definita significa verificare che se $a \equiv a' \mod H$ e $b \equiv b' \mod H$, allora $ab \equiv a'b' \mod H$. Se l'operazione è ben definita, allora è chiaramente associativa a causa dell'associatività dell'operazione di G. Inoltre $[1]$ ne è l'elemento neutro, e $[a][a^1] = [1]$ mostra che ogni classe laterale possiede una classe inversa. In altre parole, questa operazione induce sull'insieme G/H delle classi laterali sinistre una struttura di gruppo.

Vale la pena di notare che, in questo caso, l'applicazione $a \mapsto [a]$ che associa a ciascun elemento di G la propria classe laterale, è un omomorfismo di gruppi. Passiamo alla dimostrazione del teorema.

Dimostrazione. Se $a \equiv a' \mod H$ e $b \equiv b' \mod H$, allora esistono $h, k \in H$ tali che $a' = ah, b' = bk$. Se $H \lhd G$, allora

$$a'b' = ahbk = ab(b^{-1}hb)k = (ab)((b^{-1}hb)k).$$

Per la normalità di H, si ha $b^{-1}hb \in H$; ma H è un sottogruppo, quindi $(b^{-1}hb)k \in H$. In conclusione, $a'b' \in abH$, e quindi $a'b' \equiv H$.

Per mostrare il viceversa, notiamo che se l'operazione è ben definita, allora G/H con tale operazione è un gruppo, e la proiezione $\pi : a \mapsto [a]$ è un omomorfismo di gruppi. Allora il nucleo $\ker\pi = H$ è un sottogruppo normale di G. □

Chiaramente, ogni sottogruppo di un gruppo abeliano è normale.

3. Alcuni esempi di gruppi

3.1. **Gruppi ciclici e diedrali.** Le isometrie del piano formano gruppo rispetto all'operazione di composizione. Infatti, la composizione di isometrie è chiaramente un'isometria; inoltre, l'identità è isometrica, e l'inverso di ogni isometria è ovviamente ancora una isometria.

Vi sono due tipi di isometrie: quelle che conservano l'orientazione e quelle che la invertono. Un semplice teorema di algebra lineare ci informa che le isometrie del piano che conservano l'orientazione sono traslazioni e rotazioni, mentre quelle che la invertono sono delle simmetrie rispetto ad una retta.

Fissiamo un n-agono regolare nel piano, e chiamiamo D_n (rispettivamente C_n) l'insieme delle isometrie (risp. isometrie che conservano l'orientazione) che lo conservano, cioè che lo sovrappongono esattamente a se stesso. D_n e C_n contengono l'identità, e sono quindi insiemi non vuoti. Il gruppo C_n è generato dalla rotazione di $2\pi/n$ attorno al centro dell'n-agono, ed è quindi ciclico di ordine n. Il gruppo D_n si chiama *gruppo diedrale*, e contiene strettamente C_n come sottogruppo.

Proposizione 3.1. $|\,\mathrm{D}_n\,| = 2n$.

Dimostrazione. Ogni elemento di D_n è univocamente determinato dalla scelta delle immagini di due suoi vertici consecutivi. Le possibili immagini sono le coppie ordinate di vertici consecutivi dell'n-agono, che sono appunto $2n$. Questo mostra, in particolare, che D_n contiene n rotazioni ed n simmetrie. □

Sia ora ρ la rotazione in senso antiorario di $2\pi/n$, e scegliamo una simmetria $s \in \mathrm{D}_n$. I due sottogruppi $H = \mathrm{C}_n = \langle\rho\rangle$ e $K = \langle s\rangle$ si intersecano nella sola identità: infatti l'altro elemento s di K non è una rotazione. Per questo motivo il sottoinsieme HK contiene $|H||K|/|H \cap K| = 2n$ elementi, e coincide pertanto con l'intero gruppo D_n. Abbiamo così dimostrato la

Proposizione 3.2. *Gli elementi $\rho^i, \rho^i s$, dove $i = 0, 1, \dots, n-1$, formano una lista completa degli elementi di* D_n.

In particolare tutti gli elementi $\rho^i s$ sono simmetrie, dal momento che gli elementi ρ^i esauriscono tutte le rotazioni di D_n. L'operazione di gruppo in D_n si descrive in modo semplice.

Lemma 3.3. *$s\rho^i = \rho^{-i}s$ per ogni $i \in \mathbb{N}$.*

Dimostrazione. L'elemento $\rho^i s$ è una simmetria, ed ha perciò ordine 2. Questo mostra che $\rho^i s \rho^i s = e$, da cui si ottiene l'enunciato moltiplicando per ρ^{-i} a sinistra, e per s a destra. □

Si ottiene immediatamente:

Proposizione 3.4. *La composizione in D_n è tale che*

$$\begin{aligned} \rho^i \cdot \rho^j &= \rho^{i+j}, & \rho^i \cdot \rho^j s &= \rho^{i+j}s, \\ \rho^i s \cdot \rho^j &= \rho^{i-j}s, & \rho^i s \cdot \rho^j s &= \rho^{i-j}. \end{aligned}$$

Abbiamo già osservato che $\rho^n = e$, e di conseguenza, $\rho^{kn} = e$ per ogni $k \in \mathbb{Z}$. Questo mostra che per calcolare ρ^i è importante conoscere soltanto la classe di resto di i modulo n. Nella Proposizione precedente, le somme e le differenze tra esponenti vanno pertanto calcolate modulo n. E' facile, ora, determinare tutti i sottogruppi di C_n e D_n.

Proposizione 3.5. *I sottogruppi di C_n sono tutti ciclici, e precisamente della forma $\mathrm{C}_m = \langle \rho^d \rangle$, dove d ed m sono divisori di n, tali che $n = md$.*

Dimostrazione. Sia H un sottogruppo di $\mathrm{C}_n = \langle \rho \rangle$. Definiamo $E = \{i \in \mathbb{Z} \,|\, \rho^i \in H\}$. Chiaramente, $n \in E$. Inoltre E è un sottogruppo di $\mathbb{Z}$, quindi è del tipo (d), per qualche $d \in \mathbb{N}$. Dal momento che $n \in E = (d)$, allora d divide n, ed $H = \langle \rho^d \rangle$. Se $n = dm$, H è un gruppo ciclico di ordine m. □

Vale la pena di notare che, in D_n, $\langle \rho^n \rangle$ è semplicemente $\langle e \rangle$.

Proposizione 3.6. *I sottogruppi di D_n sono ciclici della forma $\langle \rho^d \rangle$, oppure diedrali della forma $\langle \rho^d, \rho^i s \rangle$, dove d è un divisore di n e $0 \leq i < d$.*

Dimostrazione. Sia H un sottogruppo di D_n. Vi sono due possibilità: H è completamente contenuto in $\mathrm{C}_n < \mathrm{D}_n$, oppure vi è qualche elemento di H che inverte l'orientazione del piano. Nel primo caso, H è un sottogruppo di C_n, ed è quindi della forma $\mathrm{C}_m = \langle \rho^d \rangle$ per la Proposizione 3.5.

Nel secondo caso, H contiene il sottogruppo $K = H \cap \mathrm{C}_n$, che è della forma $\langle \rho^d \rangle$ per un divisore opportuno d di n. La relazione di congruenza modulo K nel sottogruppo H possiede soltanto due classi di equivalenza: quella delle rotazioni e quella delle simmetrie. Infatti, se $a, b \in H$ conservano entrambe, o invertono entrambe, l'orientazione, allora $a^{-1}b \in H$ conserva l'orientazione, ed è perciò una rotazione contenuta in K. Se invece una sola tra a e b è una rotazione, allora ab^{-1} è una simmetria, e pertanto non contenuta in K.

Questo mostra che K ha indice 2 in H, e quindi H contiene $2|K| = 2n/d$ elementi. Di conseguenza H è generato da ρ^d insieme ad una qualsiasi simmetria $\rho^i s \in H$; è possibile infine fare in modo che $0 \leq i < d$ moltiplicando per un'opportuna potenza di ρ^d. □

4. Aritmetica modulare

4.1. Classi di resto modulo n.

Lemma 4.1. *Siano a, b, c elementi di $\mathbb{Z}$. Se $a|b, a|c$, allora $a|hb \pm kc$ per ogni $h, k \in A$.*

Dimostrazione. Se $a|b, a|c$, allora esistono $x, y \in A$ tali che $b = ax, c = ay$. Ma allora $hb \pm kc = h(ax) \pm k(ay) = (hx \pm ky)a$ è un multiplo di a. □

Definizione 4.2. Sia $n \in \mathbb{N}, n > 1$. Due elementi $a, b \in \mathbb{Z}$ si dicono *congrui* o *congruenti modulo n* se $n|(b-a)$. Questo fatto si indica con la notazione $a \equiv b \mod n$.

Proposizione 4.3. *La relazione di congruenza modulo n è di equivalenza.*

Dimostrazione. Si tratta della relazione di congruenza modulo il sottogruppo di $\mathbb{Z}$ costituito dai multipli di n. □

L'insieme quoziente di $\mathbb{Z}$ per la relazione di congruenza modulo n si indica con $\mathbb{Z}/(n)$.

Lemma 4.4. *$\mathbb{Z}/(n)$ contiene esattamente n elementi.*

Dimostrazione. Gli elementi $0, 1, \ldots, n-1$ appartengono a classi di equivalenza distinte, in quanto da $0 \leq a, b < n$, $a \neq b$, si ricava $0 \neq |a - b| < n$, quindi $a - b$ non può essere multiplo di n.

Per vedere che ogni elemento $a \in \mathbb{Z}$ giace in una delle classi di equivalenza $[0], [1], \ldots, [n-1]$, basta utilizzare la divisione euclidea:

$$a = nq + r, \quad 0 \leq r < n,$$

per concludere che $a \equiv r \mod n$. □

Proposizione 4.5. *Se $a \equiv a' \mod n$ e $b \equiv b' \mod n$, allora*

$$a + b \equiv a' + b' \mod n \qquad e \qquad ab \equiv a'b' \mod n.$$

Di conseguenza, le operazioni $[a] + [b] = [a + b], [a] \cdot [b] = [ab]$ sono ben definite in $\mathbb{Z}/(n)$.

Dimostrazione. Le ipotesi sono equivalenti a dire che $n|(a' - a), n|(b' - b)$. Ma allora $n|((a' - a) + (b' - b)) = (a' + b') - (a + b)$, cioè $a + b \equiv a' + b' \mod n$. Inoltre $n|(a' - a)b' + a(b' - b) = a'b' - ab$, cioè $ab \equiv a'b' \mod n$. □

Teorema 4.6. *$\mathbb{Z}/(n)$, dotato delle operazioni di somma e prodotto ereditate da $\mathbb{Z}$, è un anello commutativo con unità.*

Dimostrazione. Questo vuol dire che le operazioni di somma e prodotto sono commutative e associative, che quella di somma è un'operazione di gruppo abeliano, e che il prodotto distribuisce rispetto alla somma.

Si dimostra tutto facilmente. L'elemento neutro rispetto alla somma è $[0]$, mentre l'unità è $[1]$. L'inverso additivo di $[a]$ è chiaramente $[-a]$. □

4.2. **Identità di Bézout e algoritmo euclideo.** Abbiamo già visto che se a, b sono interi, allora il sottogruppo $(a) + (b) < \mathbb{Z}$ è generato dal massimo comun divisore $d = \mathrm{MCD}(a, b)$. Di conseguenza, d è della forma $ha + kb$, per un'opportuna scelta di $h, k \in \mathbb{Z}$. Ad esempio, $\mathrm{MCD}(25, 60) = 5$, e in effetti $5 = 5 \cdot 25 - 2 \cdot 60$. L'espressione di $d = \mathrm{MCD}(a, b)$ nella forma $d = ha + kb$ si chiama *identità di Bézout*.

Sarà in seguito importante trovare una maniera rapida per calcolare il massimo comun divisore di due interi, esprimendolo possibilmente nella forma indicata sopra. Una possibilità è quella di applicare il cosiddetto algoritmo euclideo, che vi descrivo brevemente.

Lemma 4.7 (Divisione euclidea)**.** *Se $a, b \in \mathbb{Z}$ e $b > 0$, esiste un'unica scelta di $q, r \in \mathbb{Z}$ tali che $a = bg + r$, con $0 \leq r < b$; r è detto resto della divisione di a per b.*

Proposizione 4.8. *Se $a, b > 0$ sono interi, e $a = bq + r$, allora ogni divisore comune di a e b divide anche r. In altre parole, l'insieme dei divisori comuni di a, b coincide con l'insieme dei divisori comuni di b, r.*

Dimostrazione. Se d divide sia a che b, allora divide certamente $r = 1 \cdot a + (-q) \cdot b$. Viceversa, se d divide sia b che r, allora divide sicuramente anche $a = q \cdot b + 1 \cdot r$. □

Alla luce di questo fatto, calcolare il massimo comun divisore di a e b è equivalente a calcolare il massimo comun divisore di b e r, dove r è il resto della divisione di a per b. Ad esempio, poiché $1005 = 8 \cdot 119 + 53$, si avrà $\mathrm{MCD}(1005, 119) = \mathrm{MCD}(119, 53)$. Iterando questa procedura, si ottiene:

$$\begin{aligned} 1005 &= 8 \cdot 119 + 53 \\ 119 &= 2 \cdot 53 + 13 \\ 53 &= 4 \cdot 13 + 1 \\ 13 &= 13 \cdot 1 + 0 \end{aligned}$$

e quindi $\mathrm{MCD}(1005, 119) = \mathrm{MCD}(119, 53) = \mathrm{MCD}(53, 13) = \mathrm{MCD}(13, 1) = \mathrm{MCD}(1, 0)$. I resti diventano ogni volta più piccoli, e dopo un numero finito di passi si dovrà avere un resto nullo. Si vede facilmente che $\mathrm{MCD}(n, 0) = n$ e quindi l'ultimo resto non nullo è il massimo comun divisore dei due numeri di partenza. In questo caso, $\mathrm{MCD}(1005, 119) = 1$.

Tutti i numeri che si ottengono nei vari passi dell'algoritmo euclideo appartengono al sottogruppo $(a) + (b) < \mathbb{Z}$, e possiamo utilizzare i vari passi dell'algoritmo euclideo per esprimerli esplicitamente nella forma $ha + kb$. Per semplicità di notazione, indichiamo $h \cdot 1005 + k \cdot 119$ nella forma compatta $[h, k]$. Allora

$$\begin{aligned} 1005 &= [1 : 0] \\ 119 &= [0 : 1] \\ 53 &= [1 : 0] - 8[0 : 1] = [1 : -8] \\ 13 &= [0 : 1] - 2[1 : -8] = [-2 : 17] \\ 1 &= [1 : -8] - 4[-2 : 17] = [9 : -76] \end{aligned}$$

In questo modo, abbiamo calcolato l'identità di Bézout $1 = 9 \cdot 1005 - 76 \cdot 119$. Due numeri si dicono primi tra loro se 1 è il loro massimo comun divisore. Pertanto, abbiamo appena visto come 1005 e 119 siano primi tra loro.

Corollario 4.9. *Se $a, b, c \in \mathbb{Z}$ sono interi non nulli, e $c = ha + kb$ per qualche $h, k \in \mathbb{Z}$, allora il massimo comun divisore di a e b divide c. In particolare a e b sono primi tra loro se e solo se è possibile esprimere 1 nella forma $ha + kb$ per una scelta opportuna di $h, k \in \mathbb{Z}$.*

L'identità di Bézout è di particolare utilità nello studio delle proprietà di divisibilità dei numeri primi.

Definizione 4.10. Un numero intero n si dice *primo* se non è invertibile in $\mathbb{Z}$, e in ogni fattorizzazione $n = ab$, almeno uno tra i fattori a, b è invertibile.

Osservazione 4.11. E' utile ricordare come gli unici elementi invertibili in $\mathbb{Z}$ siano 1 e -1. Segue quindi immediatamente che gli unici divisori di un numero primo p sono $\pm 1, \pm p$.

Lemma 4.12. *Sia $p \in \mathbb{Z}$ primo. Se p divide un prodotto ab di interi, allora divide almeno uno dei fattori a, b.*

Dimostrazione. Mostriamo che se p divide ab ma non divide a, allora deve necessariamente dividere b.

Sappiamo che p è primo. Essendo $\mathrm{MCD}(p, a)$ un divisore di p, può essere soltanto 1 oppure p. Ad ogni modo, $\mathrm{MCD}(p, a)$ divide anche a, e quindi non può essere p. Pertanto $\mathrm{MCD}(p, a) = 1$. Di conseguenza, è possibile scrivere 1 nella forma $ha + kp$, per un'opportuna scelta di $h, k \in \mathbb{Z}$. Ma allora $b = 1 \cdot b = (ha + kp)b = h(ab) + (kb)p$; poiché p divide sia ab che p, la divisibilità di b per p segue immediatamente. □

Un dominio d'integrità è un anello commutativo nel quale il prodotto di elementi non nulli non è mai 0. Ad esempio, $\mathbb{Z}$ è un dominio d'integrità, così come ogni campo è un dominio d'integrità.

Proposizione 4.13. *Sia $n > 1$ un numero intero. $\mathbb{Z}/(n)$ è un dominio d'integrità se e solo se n è primo.*

Dimostrazione. Se n non è primo, è allora possibile trovare $1 < a, b < n$ tali che $ab = n$. Ma allora $[a], [b] \neq [0]$ e $[a][b] = [n] = [0]$, e $\mathbb{Z}/(n)$ non può essere un campo.

Sia invece n primo. Dire che $[a][b] = [0]$ è lo stesso che richiedere che n divida ab. Ma allora n divide uno tra a e b, e quindi uno tra $[a]$ e $[b]$ coincide con $[0]$. □

5. Classi di resto invertibili e Teorema di Eulero

In questa sezione dimostriamo un enunciato più preciso di quello contenuto nella Proposizione 4.13.

Lemma 5.1. *Siano $a, n \in \mathbb{N}$ interi maggiori di 1. Allora $[a]$ è invertibile in $\mathbb{Z}/(n)$ se e solo se $(a, n) = 1$.*

Dimostrazione. Se $(a, n) = 1$, per l'identità di Bezout è possibile trovare $h, k \in \mathbb{Z}$ tali che $ah + nk = 1$. Ma allora $[a][h] = [ah] = [1]$, e quindi $[h]$ è l'inverso di a in $\mathbb{Z}/(n)$.

Viceversa, se $[a]$ possiede un inverso $[h]$ in $\mathbb{Z}/(n)$, allora $[ah] = [1]$, cioè $ah \equiv 1 \mod n$. Ma allora $ah - 1 = kn$ per qualche $k \in \mathbb{Z}$, e $(a, h) = 1$ per il Corollario 4.9. □

Teorema 5.2. *Se $p \in \mathbb{Z}$ è un numero primo, allora $Z/(p)$ è un campo.*

Dimostrazione. Se $[a]$ è una classe di resto diversa da $[0]$, allora p non divide a. In tal caso $(a, p) = 1$ e quindi $[a]$ possiede un inverso moltiplicativo. □

Il numero degli elementi invertibili in $\mathbb{Z}/(n)$ si indica con $\phi(n)$. Chiaramente $\phi(p) = p - 1$ se p è un numero primo. In tal caso, più in generale, si ha $\phi(p^n) = p^{n-1}(p - 1)$.

Osservazione 5.3. Siano $a, b, n \in \mathbb{Z}$. Condizione necessaria affinché la congruenza $ax \equiv b \mod n$ abbia soluzioni in $\mathbb{Z}$ è che il massimo comun divisore $d = (a, n)$ divida b. In effetti $ax \equiv b \mod n$ è equivalente a dire che n divide $ax - b$, cioè che $b = ax + kn$ per qualche $k \in \mathbb{Z}$. Dal momento che d divide sia a che n, divide anche i loro multipli, e quindi anche b.

Quando tale condizione necessaria è soddisfatta, possiamo scrivere $a = a'd, b = b'd, n = n'd$ per un'opportuna scelta di $a', b', n' \in \mathbb{Z}$. Allora la congruenza diventa $d(a'x - b') \equiv 0 \mod n'd$, che è equivalente a $a'x \equiv b' \mod n'$, nella quale $(a', n') = 1$. In tale situazione, il Lemma 5.1 ci assicura che a' possiede un inverso $\mod n$. Moltiplicando entrambi i membri per a'^{-1} si ottengono tutte le soluzioni della congruenza iniziale.

Questo mostra che $(a, n)|b$ è una condizione necessaria e sufficiente affinché la congruenza $ax \equiv b \mod n$ abbia soluzione.

5.1. **Il piccolo Teorema di Fermat ed il Teorema di Eulero.** Se A è un anello commutativo con unità, allora l'insieme $A^\times$ degli elementi invertibili di A è un gruppo rispetto al prodotto. Abbiamo già visto esempi di questo fatto: se K è un campo, allora $K^\times = K \setminus \{0\}$ è un gruppo rispetto alla moltiplicazione; se $A = \mathbb{Z}$, $\mathbb{Z}^\times$ coincide con $\{\pm 1\}$ che abbiamo già visto essere un gruppo rispetto al prodotto.

Gli elementi invertibili di $\mathbb{Z}/(n)$ costituiscono anch'essi un gruppo moltiplicativo, detto *gruppo degli invertibili modulo n*. Se n è primo, questo è il gruppo moltiplicativo degli elementi non nulli, ma se n non è primo, non bisogna escludere solo lo 0. Ad esempio, $\mathbb{Z}/(6)^\times = \{1, 5\}$, $\mathbb{Z}/(8)^\times = \{1, 3, 5, 7\}$, $\mathbb{Z}/(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Il numero di elementi in $\mathbb{Z}/(n)^\times$ si indica, tradizionalmente, con $\varphi(n)$. Chiaramente $\varphi(p) = p - 1$ se p è primo; si può mostrare, e non so se lo vedremo, che

$$\varphi(n) = n \cdot \prod_{p \text{ primo}, p|n} \left(1 - \frac{1}{p}\right).$$

Ad esempio,

$$\varphi(15) = 15 \cdot \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8.$$

Sappiamo che l'ordine di ogni elemento in un gruppo deve dividere l'ordine del gruppo. Nel caso particolare del gruppo $\mathbb{Z}/(n)^\times$, si ottiene:

Teorema 5.4 (Eulero)**.** *Se $(a, n) = 1$, allora $a^{\varphi(n)} \equiv 1 \mod n$.*

Questo risultato ha una conseguenza immediata:

Teorema 5.5 (Fermat)**.** *Se p è un numero primo, allora $a^p \equiv a \mod p$.*

Dimostrazione. Se p divide a, allora sia a che a^p sono $\equiv 0 \mod p$.

Se invece p non divide a, allora $(a, p) = 1$ e quindi $a^\phi(p) \equiv 1 \mod p$. Ricordando che $\varphi(p) = p - 1$ si ottiene $a^{p-1} \equiv 1 \mod p$. Moltiplicando per a, si ottiene $a^p \equiv a \mod p$. □

6. Il teorema cinese del resto

Supponiamo di dover risolvere un sistema di congruenze

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

e che m, n siano primi tra loro. E' evidente che trovata una soluzione x, anche $x + mn$ sarà una soluzione; viceversa, se x, y sono soluzioni del sistema, allora $x \equiv y$ sia $\mod m$ che $\mod n$. Poiché sia m che n dividono $y - x$, e m, n sono primi tra loro, allora mn divide $y - x$ e quindi $x \equiv y \mod n$. Le soluzioni del sistema, se ve ne sono, sono pertanto date dagli elementi di una singola classe di congruenza modulo mn. Rimane la domanda: il sistema ha soluzione per ogni scelta di a, b, oppure no?

La risposta è semplice: l'applicazione

$$\begin{array}{rcl} \mathbb{Z}/(mn) & \to & \mathbb{Z}/(m) \times \mathbb{Z}/(n) \\ [x]_{mn} & \mapsto & ([x]_m, [x]_n) \end{array}$$

è iniettiva per il discorso fatto prima, e gli insieme $\mathbb{Z}/(mn)$ e $\mathbb{Z}/(m) \times \mathbb{Z}/(n)$ hanno entrambi mn elementi. Un'applicazione iniettiva tra insieme finiti della stessa cardinalità è inevitabilmente suriettiva, e quindi ogni possibile scelta di $([a]_m, [b]_n)$ viene raggiunta.

Teorema 6.1 (cinese del resto)**.** *Siano m, n interi primi tra loro. Il sistema di congruenze*

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

ammette soluzioni per ogni scelta di a, b interi. La soluzione è unica modulo mn.

E' interessante trovare un modo concreto per risolvere il sistema di congruenze. Una maniera molto astratta è quella di usare l'identità di Bézout $1 = hm + kn$: si vede subito che $hm \equiv 0 \mod m, hm \equiv 1 \mod n$, mentre $kn \equiv 0 \mod n, kn \equiv 1 \mod m$. Inevitabilmente, $x = akn + bhm$ è la soluzione desiderata.

Alternativamente, si può scrivere $x = a + ym$ e sostituire nella seconda congruenza. Si ottiene $a + ym \equiv b \mod n$, e l'equazione $ym \equiv b - a \mod n$ si risolve facilmente in y, poiché m è primo con n e possiede quindi un inverso $\mod n$. Trovato il valore di y, lo si sostituisce in $x = a + ym$, e si trovano le soluzioni.

L'affermazione del Teorema cinese del resto è in realtà algebricamente più profonda.

Teorema 6.2 (cinese del resto II). *Poniamo sul prodotto cartesiano $\mathbb{Z}/(m) \times \mathbb{Z}/(n)$ una struttura di anello definendo operazioni di somma e prodotto componente per componente. Allora l'applicazione*

$$\begin{array}{rcl} \phi : \mathbb{Z}/(mn) & \to & \mathbb{Z}/(m) \times \mathbb{Z}/(n) \\ [x]_{mn} & \mapsto & ([x]_m, [x]_n) \end{array}$$

è un isomorfismo di anelli.

Dire che ϕ è un isomorfismo di anelli significa che $\phi(a+b) = \phi(a) + \phi(b)$ e $\phi(ab) = \phi(a)\phi(b)$, e ovviamente che ϕ è invertibile. Lo dico in un altro modo: possiamo fare i conti (somme e prodotti) indifferentemente da una parte o dall'altra e poi tradurre attraverso l'applicazione ϕ o la sua inversa, e i risultati coincidono.

6.1. **La crittografia RSA.** L'aritmetica modulare ha applicazioni semplici e interessanti alla crittografia a chiave pubblica. L'obiettivo è quello di implementare un sistema crittografico che permetta lo scambio sicuro di messaggi senza il bisogno di dover prima comunicare in modo sicuro (e segreto!) una chiave.

Il sistema RSA (Rivest, Shamir, Adleman) è una possibile implementazione[6] che utilizza le proprietà delle classi di resto. Passo immediatamente alla descrizione del sistema.

Alice, che vuole poter ricevere messaggi criptati che solo lei può decodificare, sceglie due numeri primi distinti grandi p, q e li moltiplica ottenendo $N = pq$. Sceglie poi un numero $0 < d < \varphi(N)$ primo con $\varphi(N)$ e ne calcola l'inverso h modulo $\varphi(N)$.

A questo punto, comunica pubblicamente i numeri d, N, che costituiscono la chiave pubblica. Tiene invece per se le informazioni p, q, h, che costituiscono la chiave privata.

Chi[7] voglia comunicare il messaggio $0 < x < N$ ad Alice, calcola $y = x^d \mod N$ e invia pubblicamente y. Alice ha una maniera comoda di calcolare y dato x: in effetti, calcolando y^h si ottiene

$$y^h = (x^d)^h = x^{dh} = x^{1+k\varphi(N)} \equiv x \mod N.$$

Qui abbiamo utilizzato il Teorema di Eulero, che vale soltanto se x è primo con N; ad ogni modo, quando p e q sono molto grandi, la probabilità che x sia divisibile per p o per q è trascurabile[8].

La sicurezza del sistema sta nel fatto che h è calcolabile facilmente solamente se è noto $\varphi(N) = (p-1)(q-1)$. Ad ogni modo, conoscere sia $N = pq$ che $\varphi(N)$ è equivalente a conoscere anche p e q. Tuttavia, il tempo necessario al calcolo di primi molto grandi cresce molto più lentamente del tempo necessario alla fattorizzazione dei due numeri primi — ci sono algoritmi più o meno efficienti per la verifica della primalità, ma non sono noti algoritmi efficienti che producano la fattorizzazione di un numero sicuramente non primo — e quindi è sempre possibile scegliere la taglia dei numeri p e q in modo che la fattorizzazione di pq sia infattibile.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI DI ROMA – "LA SAPIENZA"
E-mail address: dandrea@mat.uniroma1.it

[6] che non è dimostrabilmente sicura, tra l'altro!

[7] tipicamente Bob!

[8] In realtà, tutto funziona anche quando x non è primo con N: basta verificare che $x^{dh} \equiv x$ sia modulo p che modulo q. il che è essenzialmente il piccolo Teorema di Fermat.