Appunti del corso di Matematica Discreta
Corso di Laurea di base in Matematica

Norberto Gavioli

A.A. 2002/2003

Capitolo 1

Classi di resto e loro aritmetica

Prerequisiti: numeri interi, relazioni di equivalenza.

1.1 Congruenze modulo n

Riportiamo senza dimostrazione i seguenti teoremi (dal corso di Elementi di matematica)

Teorema 1.1. *Dati due numeri interi a e $b \neq 0$ esistono e sono univocamente determinati due numeri interi q ed r detti quoziente e resto della divisione di a per b soggetti alle le due condizioni:*

1. $a = bq + r$,
2. $0 \leq r < |b|$.

Teorema 1.2 (di Bezout)**.** *Dati due numeri interi a a b esiste il loro massimo comune divisore $d = \mathrm{MCD}(a, b)$ ed esistono due numeri interi x e y tali che $d = ax + by$ (con la convenzione che di porre $\mathrm{MCD}(a, 0) = a$).*

Dimostriamo invece il seguente risultato che ci sarà utile in seguito.

Lemma 1.3. *Siano a ed n due numeri interi primi tra loro e si supponga che n divida il prodotto ab dove $b \in Z$. Allora n divide b.*

Dimostrazione. Per ipotesi esiste $c \in Z$ tale che $an = nc$. Per il teorema di Bezout esistono due interi x e y tali che $1 = \mathrm{MCD}(a, n) = ax + ny$. Moltiplicando entrambi i membri per b otteniamo $b = (ab)x + ny = (nc)x + ny = n(cx + y)$, da cui la tesi. □

Definizione 1.4. Dato un intero positivo n diremo che due numeri interi a e b sono congrui modulo n e scriveremo $a \equiv b \bmod n$ se $a - b$ è divisibile per n, ovvero se esiste un numero intero h tale che $a - b = hn$.

Come già visto nel corso di elementi la relazione di congruenza modulo n è una relazione di equivalenza in $\mathbb{Z}$. Le sue classi di equivalenza sono dette classi di resto modulo n. La classe di resto dell'intero a modulo n verrà indicata con $[a]_n$ o, talvolta sottointendendo n (se n è chiaro dal contesto), con $[a]$. Scriveremo anche $a \bmod n$ per indicare il resto r della divisione di a per n.

1.1.1 Proprietà elementari delle congruenze

Ecco alcune proprietà elementari delle congruenze:

Proposizione 1.5. *Valgono le seguenti proprietà:*

1. *Se* $a \equiv a' \bmod n$ *e* $b \equiv b' \bmod n$ *allora* $a + b \equiv a' + b' \bmod n$*; equivalentemente se* $[a]_n = [a']_n$ *e* $[a]_n = [a']_n$ *allora* $[a + b]_n = [a' + b']_n$*;*

2. *se* $a \equiv a' \bmod n$ *e* $b \equiv b' \bmod n$ *allora* $ab \equiv a'b' \bmod n$*; equivalentemente se* $[a]_n = [a']_n$ *e* $[a]_n = [a']_n$ *allora* $[ab]_n = [a'b']_n$*;*

3. $a \equiv 0 \bmod n$ *se e solo se* n *divide* a *se e solo se* $[a]_n = [0]_n$*;*

4. r *è il resto della divisione di* a *per* n *se e solo se* $0 \leq r < n$ *e* $[a]_n = [r]_n$*;*

5. $(a + b) \mod n = ((a \bmod n) + (b \bmod n)) \bmod n$.

6. $(ab) \mod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$.

Dimostrazione.

1. Per ipotesi esistono $h, k \in \mathbb{Z}$ tali che $a = a' + hn$ e $b' = b + kn$. Avremo allora $a + b = a' + b' + (h + k)n$ da cui $a + b \equiv a' + b' \bmod n$.

2. Si dimostra in modo analogo al caso 1.

3. $a \equiv 0 \bmod n$ se e solo se esiste $h \in \mathbb{Z}$ tale che $a = a - 0 = hn$. Quest'ultima affermazione è equivalente a dire che n divide a.

4. Siano q ed r il quoziente ed il resto della divisione di a per n Allora $0 \leq r < n$ e $a - r = nq$ da cui $a \equiv r \bmod n$. Viceversa se $a \equiv r \bmod n$ e $0 \leq r < n$ avremo che esiste un numero intero h tale che $a - r = nh$ e $0 \leq r < n$. Dall'unicità del quoziente e del resto della divisione di a per n (Teorema 1.1) si ha che h è il quoziente ed r è il resto della divisione di a per n.

5. $((a \bmod n)+(b \bmod n)) \bmod n$, per la 4., è conqruo modulo n a $(a \bmod n) + (b \bmod n)$. Quest'ultimo numero è conqruo modulo n ad $a + b$ (per la 1.) che a sua volta è congruo a $(a + b) \bmod n$ per la 4. Poiché entrambi i membri della 5. sono tra loro congrui modulo n e sono compresi tra 0 incluso ed n escluso deduciamo (da 4.) che essi sono tra loro eguali essendo entrambi uguali al resto della divisione di $a + b$ per n.

6. La dimostrazione è analoga al punto 5. □

Alcuni commenti:

- Dai punti 1. e 2. si deduce che la classe di resto modulo n del risultato di un'espressione contenente somme e prodotti di interi (polinomiale) si può ottenere rimpiazzando in detta espressione questi interi con interi a loro congruenti modulo n;
- i punti 5. e 6. indicano che il resto della divisione per n del risultato di un'espressione contenente somme e prodotti di interi (polinomiale) si può ottenere rimpiazzando in detta espressione questi interi con interi a loro congruenti modulo n;

Proposizione 1.6. *Ci sono esattamente n classi di resto modulo n:* $[0]_n$, $[1]_n$, $\ldots$, $[n-1]_n$.

Dimostrazione. Dato un intero a si consideri il resto r della divisione di a per n. Dal punto 4. della Proposizione 1.5 si ha che $[a]_n = [r]_n$ (ovvero a ed r sono nella stessa classe di equivalenza essendo tra loro congrui modulo n). Per tanto ogni classe di resto $[a]_n$ è della forma $[r]_n$ con $0 \leq r \leq n-1$. Questo implica che le classi di equivalenza della relazione congruenza modulo n sono quelle elencate nell'enunciato. Dobbiamo ancora dimostrare che le classi elencate sono a due a due distinte (ovvero che nell'elenco non c'è la stessa classe ripetuta più volte con nomi diversi). Supponiamo che sia $[r]_n = [r']_n$ con $0 \leq r \leq r' \leq n-1$. Allora, sempre per il punto 4. della proposizione precedente, abbiamo che r ed r' sono entrambi eguali al resto della divisione di r per n. In particolare $r = r'$. □

1.1.2 Esempi

- *Stabilire se il numero* 1437894 *è divisibile per* 9. Cominciamo a notare che $10 \equiv 1 \bmod 9$ e che quindi, per la 2. della Proposizione 1.5, $10^h \equiv 1 \bmod 9$ dove h è un intero positivo. Scriviamo 1437894 nella forma $1437894 = 1 \cdot 10^6 + 4 \cdot 10^5 + 3 \cdot 10^4 + 7 \cdot 10^3 + 8 \cdot 10^2 + 9 \cdot 10 + 4 \equiv 1+4+3+7+8+9+4 = 36 \equiv 0 \bmod 9$. Dalla 3. della Proposizione 1.5 deduciamo che 9 divide 1437894. Con questo stesso metodo si può

mostrare che un numero in forma decimale è divisibile per 9 se e solo se lo è la somma di tutte le sue cifre.

- *determinare il resto della divisione di*

$$n = ((19087387)^{2432543254324} + 4 \cdot 5^{2645654634654635461})^{34567687}$$

per 10. Cominciamo con il notare che $19087387 \equiv 7 \bmod 10$. Quindi possiamo sostituire 19087387 con 7 nella determinazione della classe di resto di n. Adesso dobbiamo trovare la classe di $7^{2432543254324}$. Cominciamo a fare le potenze di 7 modulo 10

$$7^2 = 49 \equiv 9 \bmod 10,$$
$$7^3 = 7^2 \cdot 7 \equiv 9 \cdot 7 = 63 \equiv 3 \bmod 10,$$
$$7^4 = 7^3 \cdot 7 \equiv 3 \cdot 7 = 21 \equiv 1 \bmod 10.$$

e notiamo che

$$2432543254324 = 4 \cdot (608135813581)$$

pertanto $(19087387)^{2432543254324} \equiv 7^{4\cdot(608135813581)} = (7^4)^{608135813581} \equiv 1^{608135813581} = 1 \bmod 10$.

Il numero $4 \cdot 5^{2645654634654635461}$ è divisibile per 5 e per 2 ed pertanto divisibile per 10. In particolare $5^{2645654634654635461} \equiv 0 \bmod 10$. Ne concludiamo che $n \equiv (1+0)^{34567687} = 1 \bmod 10$ e pertanto 1 (Proposizione 1.5 punto 4.) è il resto della divisione di n per 10.

1.2 Congruenze lineari

Una congruenza lineare è una scrittura della forma

$$ax + b \equiv 0 \bmod n \tag{1.1}$$

dove $a \neq 0$, b ed $n > 0$ sono interi. Un intero x_0 è detto soluzione di (1.1) se $ax_0 + b \equiv 0 \bmod n$. Una congruenza lineare può non ammettere soluzioni. Ad esempio, la congruenza $2x \equiv 1 \bmod 2$ non ammette alcuna soluzione perché nessun numero pari può essere contemporaneamente dispari.

Teorema 1.7 (delle congruenze lineari)**.** *La congruenza lineare* (1.1) *ammette soluzioni se e solo se* $d = \mathrm{MCD}(a, n)$ *divide* b*. In tal caso vi sono infinite soluzioni e si trovano in tal modo: si sceglie arbitrariamente una soluzione particolare* x_0*, le soluzioni di* (1.1) *sono allora tutte e sole della forma* $x_k = x_0 + k\frac{n}{d}$ *al variare di* k *in* $\mathbb{Z}$*. L'insieme delle soluzioni è unione di* d *classi di resto modulo* n *e più precisamente di* $[x_0]_n$*,* $\ldots$*,* $[x_{d-1}]_n$*.*

Dimostrazione. Supponiamo che esista una soluzione x_0 della (1.1). Allora esiste $h \in \mathbb{Z}$ tale che $ax_0 + b = hn$. Poiché d divide tanto n che a potremo scrivere $a = a'd$ e $n = n'd$ di modo che $b = hn - ax_0 = d(hn' - a'x_0)$ risulta essere divisibile per d. Viceversa supponiamo che $b = b'd$ sia divisibile per d. Per il Teorema di Bezout possiamo scrivere $d = as + nt$ per opportuni $s, t \in Z$. Pertanto $b = b'd = b'(as + nt) = a(b's) + (b't)n$. Posto $h = nt$ e $x_o = -b's$ abbiamo mostrato che $ax_0 + b = hn$ ovvero $ax_0 + b \equiv 0 \bmod n$ pertanto la (1.1) ammette almeno una soluzione x_0.

Supponiamo ora che la congruenza lineare (1.1) ammetta una soluzione x_0. Al variare di $k \in \mathbb{Z}$ poniamo $x_k = x_0 + k\frac{n}{d}$. Mostriamo che x_k è anch'essa una soluzione di (1.1): $ax_k + b = a(x_0 + k\frac{n}{d}) + b = (ax_0 + b) + \left(k\frac{a}{d}\right) n \equiv (ax_0 + b) \equiv 0 \bmod n$. Resta quindi da vedere che ogni soluzione y di (1.1) è della forma x_k. Supponiamo che $ay + b \equiv 0 \bmod n$, allora esistono un $u, v \in \mathbb{Z}$ tali che $ay + b = un$ e $ax_0 + b = vn$. Facendo la differenza membro a membro delle due precedenti uguaglianze otteniamo $a(y - x_0) = (u - v)n$. Quindi dividendo per d si trova $a'(y - x_0) = (u - v)n'$. Poiché a' ed n' sono primi tra loro, dal Lemmma 1.3 deduciamo che n' divide $y - x_0$. Pertanto esiste $k \in Z$ tale che $y - x_0 = kn' = k(\frac{n}{d})$ e $t = x_0 + k\frac{n}{d} = x_k$ per un opportuno $k \in \mathbb{Z}$.

È chiaro che se $y \equiv x_k \bmod n$ allora anche y è una soluzione della congruenza (1.1). Dobbiamo ora mostrare che tra le soluzioni della forma x_k ve ne sono d non congrue a due a due tra loro modulo n e non di più.

Infatti $x_k \equiv x_h \bmod n$ se e solo esiste $s \in \mathbb{Z}$ tale che $sn = x_k - x_h = x_0 + k\frac{n}{d} - x_0 - h\frac{n}{d} = (k - h)\frac{n}{d}$, ovvero se solo se esiste un intesro s tale che $sd = k - h$ che equivale a scrivere $k \equiv h \bmod d$. Pertanto le classi di resto modulo n individuate dalle soluzioni della (1.1) sono tante quante le classi di resto modulo d, ovvero d. Queste soluzioni sono tutte congrue modulo n ad una ed una sola delle seguenti: $x_0, \ldots, x_{d-1}$. □

Definizione 1.8. Un intero a è detto invertibile modulo n (ove $n \neq 0$) se esiste un intero x tale che $ax \equiv 1 \bmod n$. Se esiste tale intero x viene detto inverso di a modulo n.

Corollario 1.9. *Un intero a è invertibile modulo b se solo se* $\mathrm{MCD}(a, n) = 1$. *In tal caso gli inversi di a modulo n formano una (sola) classe di resto modulo n.*

Dimostrazione. Notiamo che a è invertibile modulo n se e solo se la congruenza lineare $ax - 1 \equiv 0 \bmod n$ ammette una soluzione. Per il Teorema 1.7 questo avviene esattamente quando il massimo comune divisore tra a ed n divide 1 e pertanto $d = \mathrm{MCD}(a, n) = 1$. In tal caso, sempre per lo stesso teorema, le soluzioni sono della forma $x_k = x_0 + kn$, al variare di k in $\mathbb{Z}$, e pertanto sono esattamente gli elementi della classe di resto modulo n di x_0. □

1.2.1 Soluzione delle congruenze lineari: esempi

- *Determinare, se esistono, le soluzioni della congruenza lineare* $52x + 12 \equiv 0 \bmod 128$. Cominciamo a notare che $4 = \text{MCD}(128, 52)$ divide il *termine noto* 12. Pertanto esistono infinite soluzioni. Vediamo ora come determinarle. Notiamo che $52x + 12 \equiv 0 \bmod 128$ se e solo se esiste $h \in \mathbb{Z}$ tale che $52x + 12 = 128h$ se e solo se se esiste $h \in \mathbb{Z}$ tale che $13x + 3 = 32h$ ovvero se e solo $13x + 3 \equiv 0 \bmod 32$. Risolviamo allora quest'ultima congruenza: notiamo che in questo caso il massimo comune divisore tra il coefficiente della x ed il modulo è $\text{MCD}(13, 32) = 1$. Per il teorema di Bezout esistono due interi u e v (determinabili con l'algoritmo di Euclide) tali che $1 = 13u + 32v$. Ad esempio, vanno bene $u = 5$ e $v = -2$. Scriviamo $-13u + 1 = 32v$ e moltiplichiamo entrambi i membri per 3. Otteniamo $13 \cdot (-3u) + 3 = (32 \cdot 3)v \equiv 0 \bmod 32$. Pertanto scegliendo $x_0 = -3u = -15$ abbiamo $13x_0 + 3 \equiv 0 \bmod 32$ e pertanto x_0 è una soluzione particolare della nostra congruenza iniziale. Tutte le altre soluzioni sono della forma $x_k = -15 + 32k$ al variare di k in $\mathbb{Z}$. Modulo 128 queste si ripartiscono in quattro classi di resto: $[17]_{128}$, $[49]_{128}$, $[81]_{128}$ e $[113]_{128}$

- *Stabilire quali tra i numeri* $1, -7, 3, 11$ *sono invertibili modulo* 12*; per questi determinare gli inversi modulo* 12. L'intero 1 è sempre invertibile modulo n ed ammette se stesso come inverso. Gli inversi di 1 sono tutti e soli della forma $x_k = 1 + 12k$. Il numero -7 è primo con 12 pertanto è invertibile modulo 12. I suoi inversi formano una classe di resto modulo 12. pertanto tra essi ve ne è uno x compreso tra 1 e 11 che soddisfa la congruenza $-7x - 1 \equiv 5x - 1 \equiv 0 \bmod 12$. Provando tutti i numeri tra 1 e 11 vediamo che $x = 5$ è una soluzione infatti $(-7) \cdot 5 = -35 \equiv 1 \bmod 12$. Gli altri inversi sono tutti e soli i numeri della forma $x_k = 5 + 12k$. Il numero 3 non è primo con 12 e pertanto non è invertibili modulo 12. Il numero 11 è congruo a -1 modulo 12 e quest'ultimo ammette come inverso se stesso modulo 12. Pertanto 11 ammette sé stesso come inverso modulo 12. Gli altri inversi sono della forma $x_k = 11 + 12k$ (tra cui figura appunto -1).

1.2.2 Esercizi

Esercizio 1.1. Determinare ove possibile tutte le soluzioni di ciascuna delle seguenti congruenze lineari:

1. $3x + 7 \equiv 0 \bmod 43$,
2. $12x + 4 \equiv 0 \bmod 16$,

3. $1242x + 4 \equiv 0 \bmod 26$,

4. $125x + 1 \equiv 0 \bmod 126$.

Esercizio 1.2. Calcolare, se esiste

1. l'inverso di 11 modulo 13,

2. l'inverso di 16 modulo 55,

3. l'inverso di 11 modulo 22,

4. l'inverso di n modulo $n + 1$, (dove $n \geq 1$)).

1.3 Operazioni tra classi di resto

L'insieme delle classi di resto modulo n viene solitamente denotato con $\mathbb{Z}_n$ o con $\mathbb{Z}/n\mathbb{Z}$. Noi adotteremo la prima notazione per motivi di brevità. Il sottoinsieme delle classi di resto diverse dalla classe $[0]_n$ sarà denotato con $\mathbb{Z}_n^*$.

Date due classi di resto $[a]_n$ e $[b]_n$ se ne può definire la somma ed il prodotto nel seguente modo;

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

$$[a]_n \cdot [b]_n = [ab]_n.$$

I punti 1. e 2. della Proposizione 1.5 garantiscono che la definizione è ben posta e non dipende dai rappresentanti a e b delle classi. Per essere chiari se si sceglie un'altra coppia di interi a' e b' tale che $[a]_n = [a']_n$ e $[b]_n = [b']_n$ allora $[a + b]_n = [a' + b']_n$ e lo stesso vale per l'operazione di prodotto.

Le operazioni che abbiamo introdotto permettono di sommare e moltiplicare classi di resto ottenendo come risultati ancora classi di resto.

Le dimostrazioni delle proprietà che seguono sono immediate e sono lasciate allo studente quale esercizio.

1.3.1 Proprietà della somma

Comunque scelti tre interi a, b e c si ha:

- **proprietà associativa**: $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$,
- **proprietà commutativa**: $[a]_n + [b]_n = [b]_n + [a]_n$,

- **elemento neutro o zero**: $[a]_n + [0]_n = [0]_n + [a]_n = [a]_n$,
- **elemento opposto** $[a]_n + [-a]_n = [-a]_n + [a]_n = [0]_n$.

L'elemento $[-a]_n$ viene usualmente denotato con $-[a]_n$. In tal modo si può definire per un intero m la classe $m[a]_n$ che porremo uguale a $\sum_{i=1}^{m}[a]_n = [ma]_n$ se m è positivo, uguale a $\sum_{i=1}^{-m} -[a]_n = [ma]_n$ se m è negativo.

1.3.2 Proprietà del prodotto

- **proprietà associativa**: $([a]_n \cdot [b]_n) \cdot [c]_n = [a]_n \cdot ([b]_n \cdot [c]_n)$,
- **proprietà commutativa**: $[a]_n \cdot [b]_n = [b]_n \cdot [a]_n$,
- **elemento neutro o zero**: $[a]_n \cdot [1]_n = [1]_n \cdot [a]_n = [a]_n$,
- **elemento inverso** se $\mathrm{MCD}(a, n) = 1$ allora esiste un intero b (b è un qualsiasi inverso di a modulo n) tale che $[a]_n \cdot [b]_n = [b]_n \cdot [a]_n = [1]_n$. In tal caso si dice che la classe di resto $[a]_n$ è invertibile ed ammette la classe $[b]_n$ come inversa. Tale classe viene usualmente denotata con $[a]_n^{-1}$

Se $[a]_n$ è una classe di resto invertibile invertibile è convenzione porre $[a]_n^{-t} = ([a]_n^{-1})^t$ per ogni intero positivo t. In tal modo valgono le usuali proprietà delle potenze anche per le classi di resto.

1.3.3 Proprietà miste

- **proprietà distributiva**: $([a]_n + [b]_n) \cdot [c]_n = [a]_n \cdot [c]_n + [b]_n \cdot [c]_n$,

1.4 L'insieme $G(n)$ delle classi di resto invertibili modulo n.

Il sottoinsieme di $\mathbb{Z}_n$ formato dalle classi invertibili modulo n viene denotato con $G(n)$.

1.4.1 La funzione φ di Eulero

La cardinalità dell'insieme $G(n)$ viene denotata con $\varphi(n)$ e la funzione $\varphi\colon \mathbb{N} \to \mathbb{N}$ così definita viene usualmente chiamata funzione φ di Eulero: $\varphi(n)$, in base al Corollario 1.9, è uguale al numero degli interi positivi minori (od eguali) ad n primi con n.

Un'altra funzione importante è la cosiddetta funzione di Moebius $\mu\colon \mathbb{N} \to \mathbb{Z}$. Se n è un numero divisibile per il quadrato c^2 di un intero $c > 1$ allora si pone $\mu(n) = 0$. Altrimenti $n = p_1 \cdots p_k$ si può scrivere come prodotto di $k \geq 0$ primi distinti (se $n = 1$ si pone $k = 0$): in tal caso n viene detto libero da quadrati e si pone $\mu(n) = (-1)^k$.

Supponiamo ora che n sia un generico numero naturale con la seguente fattorizzazione: $n = p_1^{e_1} \cdots p_k^{e_k}$ (con $e_i > 0$ per $i = 1, .., k$). Considerando che se d è un divisore non libero da quadrati di n allora $\mu(d) = 0$ si trova:

$$(1 - p_1^a) \cdots (1 - p_k^a) = \sum_{d|n} \mu(d) d^a \tag{1.2}$$

con la convenzione che il prodotto a sinistra è uguale ad 1 se $k = 0$ (ovvero $n = 1$). Se $n > 1$ ed $a = 0$ il membro di sinistra della (1.2) è uguale a zero, trovamo quindi:

$$\sum_{d|n} \mu(d) = 0 \text{ se } n > 0 \tag{1.3}$$

Sia ora $f\colon \mathbb{N} \to \mathbb{C}$ una funzione. Si definisca una nuova funzione $F\colon \mathbb{N} \to \mathbb{C}$ a partire da f tramite la formula $F(n) = \sum_{d|n} f(d)$. La funzione di Moebius permette di rideterminare f a partire da F.

Teorema 1.10 (Formula di inversione di Moebius)**.** *Con le notazioni appena introdotte si ha*

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Dimostrazione. $\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{h|\frac{n}{d}} f(h) = \sum_{(hd)|n} \mu(d) f(h) = \sum_{h|n} f(h) \sum_{d|\frac{n}{h}} \mu(d)$. Per la (1.3) nell'ultmo membro la sommatoria più interna è non nulla solo se $n/h = 1$ e pertanto l'ultima espressione è uguale a $\sum_{h=n} f(h) = f(n)$. □

Proposizione 1.11. *Per ogni numero naturale n vale l'uguaglianza*

$$n = \sum_{d|n} \varphi(d)$$

Dimostrazione. Si condiderino le frazioni aventi denominatore n e numeratore compreso tra 1 ed n:

$$\left\{ \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n} \right\}$$

Una volta ridotte queste frazioni ai minimi termini, ovvero nella forma $\frac{k}{d}$ dove k e d sono primi tra loro e $1 \leq k \leq d$, notiamo che le frazioni che hanno

denominatore d hanno per numeratore un qualsiasi numero k primo con d e minore od eguale a d: pertanto di queste ve ne sono $\varphi(d)$. Poiché le frazioni scritte sono in numero di n e, per ogni divisore d di n, quelle che ridotte ai minimi termini hanno d come numeratore sono in numero di $\varphi(d)$ troviamo $n = \sum_{d|n} \varphi(d)$. □

Proposizione 1.12. *Per ogni numero naturale n la cui fattorizzazione è $n = p_1^{e_1} \cdots p_k^{e_k}$ (con $e_i > 0$ per $i = 1, .., k$) si ha*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Dimostrazione. Si ponga $f(n) = \varphi(n)$. Con le nostre notazioni per la Proposizione 1.12 si ha $F(n) = \sum_{d|n} f(d) = \sum_{d|n} \varphi(d) = n$. Per tanto per la formula di inversione di Moebius si trova

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}. \tag{1.4}$$

Inoltre ponendo $a = -1$ nell'equazione (1.2) si trova:

$$\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) = \sum_{d|n} \mu(d)d^{-1}.$$

Moltiplicando entrambi i membri per n otteniamo:

$$n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) = \sum_{d|n} \mu(d)\frac{n}{d}. \tag{1.5}$$

La tesi segue confrontando la (1.4) e la (1.5). □

1.4.2 Ordine moltiplicativo di una classe di resto invertibile

Lemma 1.13. *Il prodotto di due classi $[a]_n$ e $[b]_n$ invertibili modulo n è ancora una classe invertibile. La classe inversa di $[a]_n \cdot [b]_n$ è $[b]_n^{-1} \cdot [a]_n^{-1}$.*

Dimostrazione. $([a]_n \cdot [b]_n) \cdot ([b]_n^{-1} \cdot [a]_n^{-1}) = [a]_n \cdot ([b]_n \cdot [b]_n^{-1}) \cdot [a]_n^{-1} = [a]_n \cdot [1]_n \cdot [a]_n^{-1} = [1]_n$. □

Lemma 1.14. *Se $[a]_n$ è una classe invertibile allora esiste un intero $t > 0$ tale che $[a]_n^t = [1]_n$.*

Dimostrazione. Consideriamo gli elementi $[a]_n^i$ al variare di i tra i numeri interi positivi. Poiché ci sono n classi di resto modulo n questi elementi non possono essere tutti tra loro distinti. Esisteranno pertanto due indici due numeri positivi $h > k > 0$ tali che $[a]_n^h = [a]_n^k$. Moltiplicando entrambi i membri per $([a]_n^{-1})^h$ otteniamo $[1]_n = [a]_n^{k-h}$. La tesi si ottiene ponendo $t = k - h$. □

Definizione 1.15. L'ordine o periodo moltiplicativo di una classe di resto invertibile $[a]_n$ indicato con $o([a]_n)$ è il minimo intero positivo t tale che $[a]_n^t = [1]_n$. Il numero $o([a]_n)$ viene anche detto ordine di a modulo n.

Proposizione 1.16. *Sia $[a]_n$ una classe invertibile modulo n e t il suo periodo moltiplicativo. Se s è un numero intero tale che $[a]_n^s = [1]_n$ allora t divide s.*

Dimostrazione. Siano q ed r il quoziente ed il resto della divisione di s per t: ovvero $s = qt + r$ ove $0 \leq r < t$. Allora $[a]_n^r = [a]_n^{s-qt} = [a]_n^s \cdot ([a]_n^t)^{-q} = [1]_n$. Poiché per definizione di periodo t è il più piccolo tra gli interi positivi u tali che $[a]_n^u = [1]_n$ e poiché $0 \leq r < t$ si deduce che $r = 0$. □

Lemma 1.17. *Sia $[a]_n$ una classe invertibile modulo n. Allora la funzione $f\colon G(n) \to G(n)$ definita da $f([x]_n) = [ax]_n$ è biunivoca.*

Dimostrazione. Notiamo che effettivamente il codominio di f è G_n. Infatti, per il Lemma 1.13, la classe $f([x]_n) = [ax]_n = [a]_n[x]_n$ è invertibile. Inoltre f è iniettiva. Infatti se supponiamo $f([x]_n) = f([y]_n)$ troviamo $[a]_n[x]_n = [a]_n[y]_n$. Moltiplicando entrambi i membri per la classe inversa di $[a]_n$ (che esiste per ipotesi) troviamo $[x]_n = [y]_n$. Ricordando che una funzione iniettiva di un insieme in sé stesso è anche suriettiva otteniamo l'asserto. □

Teorema 1.18 (di Eulero)**.** *Se a è un numero intero primo con n si ha $a^{\varphi(n)} \equiv 1 \bmod n$.*

Dimostrazione. Si definisca f come nel Lemma 1.17. Allora il prodotto π di

tutti gli elementi di $G(n)$ può essere scritto in due modi diversi:

$$\begin{aligned}
\pi &= \prod_{[x]_n \in G(n)} [x]_n \\
&= \prod_{[x]_n \in G(n)} f([x]_n) \\
&= \prod_{[x]_n \in G(n)} [ax]_n \\
&= \prod_{[x]_n \in G(n)} [a]_n [x]_n \\
&= [a]_n^{\varphi(n)} \prod_{[x]_n \in G(n)} [x]_n \\
&= [a]_n^{\varphi(n)} \pi.
\end{aligned}$$

Moltiplicando il primo e l'ultimo membro della precedente catena di uguaglianze per π^{-1} (che esiste per il Lemma 1.13) troviamo $[1]_n = [a]_n^{\varphi(n)} = [a^{\varphi(n)}]_n$ ovvero $a^{\varphi(n)} \equiv 1 \bmod n$. □

Esercizio 1.3. Determinare l'ordine moltiplicativo di 17 modulo 25 (usare il teorema di Eulero ed e la Proposizione 1.16). (**R.** 20)

Esercizio 1.4. Siano n un numero dispari ed $[a]_n$ una classe invertibile modulo n avente periodo dispari $t = 2k + 1$. Dimostrare che esiste un intero b tale che $b^2 \equiv a \bmod n$. (Sugg. notare che $[a^{k+1}]_n^2 = [a]_n^{2k+2} = [a]_n^{2k+1}[a]_n = [a]_n$).

Esercizio 1.5. Siano $n \neq 0$ un numero naturale, $[a]_n$ una classe invertibile modulo n ed m un intero tale che $(m, \varphi(n)) = 1$. Dimostrare che esiste un intero b tale che $b^m \equiv a \bmod n$. (Sugg. notare che esistono $x, y \in \mathbb{Z}$ tali che $1 = xm + y\varphi(n)$ e scrivere $a = a^{xm+y\varphi(n)} \equiv_n \ldots$).

Esercizio 1.6. Siano $n \neq 0$ un numero naturale, $[a]_n$ una classe invertibile modulo n ed m un intero tale che $(m, \varphi(n)) = 1$. Dimostrare che esiste un intero u tale che $(a^m)^u \equiv a \bmod n$.

1.4.3 Classi di resto modulo un numero primo

Teorema 1.19. *Le classi di resto modulo n diverse dalla classe $[0]_n$ sono tutte invertibili modulo n se e solo se n è un numero primo. In particolare se p è un numero primo $\mathbb{Z}_p^* = G(p)$.*

Dimostrazione. Supponiamo che le classi di resto modulo n diverse dalla classe $[0]_n$ siano tutte invertibili modulo n allora. Queste classi sono le classi

dei numeri $1, \ldots, n-1$ e pertanto, per il Corollario 1.9, si ha che questi numeri sono tutti primi con n. In particolare n ha come divisori positivi solo 1 ed n ed è quindi un numero primo.

Viceversa supponiamo che n sia un numero primo. Allora i numeri $1, \ldots, n-1$ che rappresentano le classi di resto diverse da $[0]_n$ sono primi con n e pertanto dette classi sono invertibili in virtù del corollario citato. □

Teorema 1.20 (Piccolo teorema di Fermat)**.** *Se p è un numero primo allora per ogni numero intero intero a si ha $a^p \equiv a \bmod p$.*

Dimostrazione. Notiamo che banalmente vale $a^p \equiv a \equiv 0 \bmod p$ se $a \equiv 0 \bmod p$. Possiamo pertanto supporre che a sia invertibile modulo p. Notando che $\varphi(p) = p - 1$ dal Teorema di Eulero segue che $a^{p-1} \equiv 1 \bmod p$. Moltiplicando entrambi i membri della precedente congruenza per a troviamo il nostro asserto. □

Esercizio 1.7 (Teorema di Wilson)*.* Dimostrare che se p è un numero primo allora $\prod_{[a]_p \neq [0]_p} [a]_p = [-1]_p$. (Sugg.: iniziare a dimostrare che $[a]_p \neq [a]_p^{-1}$ se e solo se $[a]_p \neq [\pm 1]_p$, dopodiché eseguire la produttoria cominciando a moltiplicare ogni classe $[a]_p \neq [\pm 1]_p$ per la propria inversa...)

1.5 Teorema cinese dei resti

Supponiamo che il numero intero $n = n_1 \cdots n_k$ sia prodotto di k fattori a due a due primi tra loro: $\mathrm{MCD}(n_i, n_j) = 1$ per $i \neq j$. Consideriamo la funzione $\psi \colon \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ definita da

$$\psi([a]_n) = ([a]_{n_1}, \ldots, [a]_{n_k}) \tag{1.6}$$

che associa alla classe di resto di a modulo n la k-upla delle classi di resto di a modulo n_1, a modulo n_2, ..., a modulo n_k. Questa funzione è ben definita e non dipende dalla scelta del rappresentante a della classe di resto $[a]_n$, infatti se $a \equiv a' \bmod n$ a maggior ragione $a \equiv a' \bmod n_i$ per $i = 1, \ldots, k$.

Teorema 1.21 (Teorema cinese dei resti prima forma)**.** *La funzione ψ definita in* (1.6) *è biunivoca.*

Dimostrazione. Poiché il dominio ed il codominio di ψ hanno la stessa cardinalità, è sufficiente mostrare che ψ è iniettiva.

Supponiamo che $\psi([a]_n) = \psi([b]_n)$ allora $a \equiv b \bmod n_i$ per $i = 1, \ldots, k$. Poiché $a - b$ è divisibile per tutti i fattori n_i di n che sono a due a due primi tra loro se ne conclude che $a - b$ deve essere divisibile per n. Pertanto $[a]_n = [b]_n$. Questo mostra che ψ è una funzione iniettiva. □

Teorema 1.22 (Teorema cinese dei resti seconda forma)**.** *Per ogni k-upla* $(n_1, \ldots, n_k)$ *di interi positivi a due a due primi tra loro e per ogni k-upla* $(a_1, \ldots, a_k)$ *di numeri interi esistono infinite soluzioni del sistema di congruenze*

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ \quad \vdots \quad \vdots \quad \vdots \quad \vdots \qquad \text{(S)}. \\ x \equiv a_k \bmod n_k \end{cases} \tag{1.7}$$

Le soluzioni di detto sistema formano una classe di resto modulo $n = n_1 \cdots n_k$.

Dimostrazione. Basta notare che se a è una soluzione del sistema (S), allora $[a]_n = \psi^{-1}([a_1]_{n_1}, \ldots, [a_k]_{n_k})$. Tale classe $[a]_n$ esiste ed è unica per il Teorema 1.21. □

1.5.1 Metodi per la soluzione di sistemi di congruenze lineari

Supponiamo di essere nelle ipotesi del Teorema 1.22 sappiamo allora che il sistema 1.7 ammette infinite soluzioni, ma non abbiamo ancora visto nessuno strumento per determinarle. Illustreremo due metodi classi per la sua risoluzione: i metodi di Newton e di Lagrange.

Metodo di Newton

Questo metodo determina ricorsivamente una soluzione x_s per le prime s congruenze del sistema 1.7 una volta che sia nota una soluzione x_{s-1} che soddisfi le prime $s-1$ congruenze del medesimo. La soluzione del sistema sarà allora x_k.

Si supponga che x_{s-1} sia nota e si ponga $x_s = x_{s-1} + t_s n_1 \cdots n_{s-1}$, dove t_s è un numero intero da determinare. È immediato verificare che x_s soddisfa le prime $s-1$ congruenze del sistema 1.7 indipendentemente dal valore assunto dalla variabile t_s. Determiniamo allora t_s imponendo che x_s soddisfi la s-esima congruenza $x_s \equiv a_s \bmod n_s$, ovvero:

$$(n_1 \cdots n_{s-1})t_s + (x_{s-1} - a_s) \equiv 0 \bmod n_s$$

Questa congruenza lineare ha una soluzione in quanto $\mathrm{MCD}((n_1 \cdots n_{s-1}), n_s)$ è uguale a 1.

Mostriamo con un esempio quanto appena spiegato. Supponiamo di voler risolvere il sistema:

$$\begin{cases} x \equiv 3 \bmod 5 \\ x \equiv 4 \bmod 14 \\ x \equiv 11 \bmod 17 \end{cases}$$

In questo esempio $n_1 = 5$, $n_2 = 14$ $n_3 = 17$ e questi tre numeri sono a due a due primi tra loro e pertanto il sistema ammette soluzione. Possiamo scegliere $x_1 = 3$ uguale al termine

noto della prima congruenza. Dopodiché si pone $x_2 = x_1 + n_1 t_2 = 3 + 5t_2$ e si impone a x_2 di soddisfare la seconda congruenza:

$$3 + 5t_2 \equiv 4 \bmod 14$$

che si può riscrivere nella forma

$$5t_2 \equiv 1 \bmod 14.$$

Ne consegue che t_2 è un inverso di 5 modulo 14. Provando successivamente a sostituire i valori 1, 2, ... nell'incognita t_2, si trova subito che $t_2 = 3$ soddisfa la nostra richiesta. Pertanto $x_2 = x_1 + 5t_2 = 3 + 15 = 18$ è una soluzione delle prime due congruenze.

Procediamo ora ponendo $x_3 = x_2 + n_1 n_2 t_3 = 18 + 70t_2$. Poiché x_3 soddisfa le prime due congruenze, determiniamo t_3 in modo che x_3 soddisfi la terza congruenza del sistema: $x_3 = 18 + 70t_3 \equiv 11 \bmod 17$. Riducendo i vari coefficienti modulo 17 e portando il termine noto a secondo membro, questa congruenza si può scrivere nella forma:

$$2t_3 \equiv 10 \bmod 17$$

L'inverso di 2 (che è il coefficiente di t_3) modulo 17 è 9. Moltiplichiamo allora per 9 entrambi i membri ottenendo $18t_3 \equiv 90 \bmod 17$. Riducendo successivamente i coefficienti modulo 17 troviamo:

$$t_3 \equiv 5 \mod 17.$$

Possiamo allora scegliere $t_3 = 5$ ed ottenere $x = x_3 = 18 + 70t_3 = 368$ come soluzione particolare del sistema. Per il Teorema 1.22 le soluzioni del sistema proposto formano la classe di resto $[368]_{1190}$, ovvero sono tutte e sole i numeri interi della forma $368 + 1190h$ al variare di h in $\mathbb{Z}$.

Metodo di Lagrange

Si inizia con il porre $N_i = n/n_i = \prod_{j \neq i} n_j$ e si nota che $\mathrm{MCD}(N_1, \ldots, N_k) = 1$. Dal Teorema di Bezout si deduce che esistono degli interi $e_1, \ldots, e_k$ tali che $\sum_{i=1}^{k} e_i N_i = e_1 N_1 + \cdots + e_k N_k = 1$. Da questa uguaglianza, notando che $N_j \equiv 0 \bmod n_i$ per $i \neq j$, si trova che $N_i e_i \equiv 1 \bmod n_i$ e $N_i e_i \equiv 0 \bmod n_j$ per $j \neq i$ Si pone allora

$$x = \sum_{i=1}^{k} a_i e_i N_i = a_1 e_1 N_1 + \cdots + a_k e_k N_k$$

cosicché $x \equiv a_i (e_i N_i) \equiv a_i \bmod n_i$. Pertanto x è una soluzione del sistema (1.7).

Come esempio riprendiamo lo stesso sistema di prima e risolviamolo con il metodo di Lagrange. Abbiamo $N_1 = n_2 n_3 = 238$, $N_2 = n_1 n_3 = 85$ e $N_3 = n_1 n_2 = 70$. Con l'algoritmo di Euclide possiamo scrivere $17 = \mathrm{MCD}(N_1, N_2) = -N_1 + 3N_2$ e quindi $1 = \mathrm{MCD}(N_1, N_2, N_3) = \mathrm{MCD}(\mathrm{MCD}(N_1, N_2), N_3) = \mathrm{MCD}(17, N_3) = 33 \cdot 17 - 8N_3 = 33(-N_1 + 3N_2) - 8N_3 = -33N_1 + 99N_2 - 8N_3$. Una soluzione particolare è allora $x = -33 \cdot 5 \cdot N_1 + 99 \cdot 4 \cdot N_2 - 8 \cdot 11 \cdot N_3 = 3938$. Riducendo modulo $n = 1190$ si può scegliere $x = 368 = 3938 \bmod 1190$.

1.5.2 Calcolo esplicito della funzione φ di Eulero tramite il teorema cinese dei resti

Torniamo ancora a considerare la funzione ψ definita in 1.6. Poiché il massimo comune divisore $\mathrm{MCD}(a, n)$ è uguale a 1 se e solo se per ogni i si ha

$\mathrm{MCD}(a, n_i) = 1$ e poiché ψ è biunivoca si trova che ψ realizza una biiezione tra l'insieme $G(n)$ delle classi invertibili modulo n e l'insieme $G(n_1) \times \cdots \times G(n_k)$ delle k-uple la cui i esima coordinata è una classe invertibile modulo n_i. Pertanto se n è uguale al prodotto di k interi $n_1, \ldots, n_k$ a due a due primi tra loro, si ha $\varphi(n) = |G(n)| = |G(n_1)| \cdots |G(n_k)| = \varphi(n_1) \cdots \varphi(n_k)$.

Cominciamo quindi a calcolare $\varphi(p^s)$ dove $s \geq 1$ è un intero e p è un numero primo. Notiamo che ci sono p^{s-1} multipli di p minori od uguali a p^s pertanto il numero degli interi positivi minori di p^s e primi con p^s è $\varphi(p^s) = p^s - p^{s-1} = p^s \left(1 - \frac{1}{p}\right)$. Supponiamo ora che $n = p_1^{s_1} \cdots p_k^{s_k}$ sia la scomposizione in fattori primi distinti di n. Per quanto detto sopra si avrà:

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{s_1}) \cdots \varphi(p_k^{s_k}) \\ &= p_1^{s_1} \left(1 - \frac{1}{p_1}\right) \cdots p_k^{s_k} \left(1 - \frac{1}{p_k}\right) \\ &= n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right). \end{aligned}$$

1.5.3 Esercizi

Esercizio 1.8. Risolvere ove possibile i seguenti sistemi di congruenze:

1. $\begin{cases} x \equiv 1 \bmod 11 \\ x \equiv 3 \bmod 5 \\ x \equiv 5 \bmod 9 \end{cases}$
2. $\begin{cases} x \equiv 7 \bmod 22 \\ x \equiv 3 \bmod 7 \\ x \equiv 5 \bmod 15 \end{cases}$
3. $\begin{cases} x \equiv 7 \bmod 22 \\ x \equiv 3 \bmod 7 \\ x \equiv 5 \bmod 15 \\ x \equiv 3 \bmod 17 \end{cases}$

Esercizio 1.9. Formalizzare e risolvere in termini di congruenze il seguente quesito.

Ieri era martedì e Marco era con me al ristorante "Da Gigi". Avevamo scommesso una cena di pesce cucinata da Gigi sul fatto che quel giorno Gigi fosse o meno in cucina. Gigi non c'era ed io ho vinto la scommessa. Gigi è un cuoco famoso e, poichè è sempre preso dai concorsi culinari, viene a cucinare personalmente solo ogni 5 giorni, lasciando che negli altri se ne occupi il suo assistente apprendista. Oggi ho telefonato al ristorante e mi ha risposto Gigi. Gli ho chiesto di prenotare un tavolo per il primo venerdì in cui ci saremmo stati sia Marco che io... che Gigi (a cucinare) naturalmente! Gigi, che sa che vengo al ristorante ogni tre giorni e che invece Marco viene ogni quattro giorni, mi ha prontamente risposto: — Ci vediamo tra x giorni! — Purtroppo un rumore dalle cucine ha coperto il famigerato x. Io mi vergogno a richiederlo a Gigi: so che mi prenderebbe in giro per mesi perchè sono negato anche per i conti più semplici. Vi chiedo di aiutarmi a calcolarlo. Ci vuole proprio una laurea in matematica?

Capitolo 2

Permutazioni su di un insieme finito

Prerequisiti dal corso di elementi di matematica: definizione di permutazione su di un insieme. Composizione di permutazioni. Definizione di permutazione inversa.

2.1 Forma ciclica di una permutazione

Supponiamo che X sia un insieme finito di cardinalità n. Possiamo quindi denotare i suoi elementi con i numeri interi compresi tra 1 ed n (è un modo come un altro di dare un nome agli elementi dell'insieme X). L'insieme delle permutazioni su X viene denotato con $S(X)$ o con S_n se $X = \{1, \ldots, n\}$. Supponiamo inoltre che sia data una permutazione $\sigma\colon X \to X$ in S_n (funzione biunivoca di X in sé). Possiamo descrivere questa funzione disegnando su di un foglio i numeri da 1 ad n e delle frecce tra questi: una freccia avrà origine in i e termine in j se $\sigma(i) = j$. Facciamo un esempio (si veda la figura 2.1).

Supponiamo che $X = \{1, 2, 3, 4, 5, 6\}$ e che σ sia la permutazione che in forma tabellare si scrive come $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 4 & 6 \end{smallmatrix}\right)$ che quindi manda 1 in 3, 2 in 5, 3 in 1, 4 in 2, 5 in 4 e fissa 6. È facile vedere che in ogni elemento di X c'è sempre una freccia che entra ed una che esce. Partendo da elemento di X e seguendo le frecce si descrive un percorso che dopo un numero finito di passi torna all'elemento di partenza. In tal modo ogni permutazione può essere descritta da un numero finito di *cicli* disgiunti. Si usa la convenzione di non riportare nella descrizione di una permutazione i cicli che contengono solo un elemento (il ciclo (6) nell'esempio in figura). Nell'esempio in questione $\sigma = (1, 3)(2, 5, 4)$. Gli elementi tra parentesi sono quelli che compaiono nei

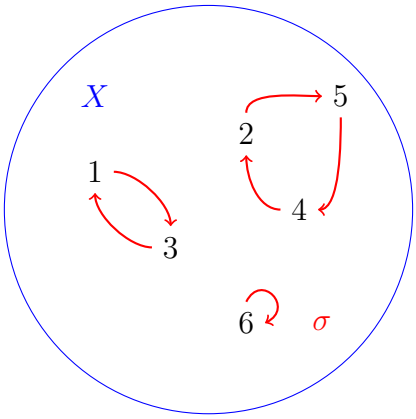


Figura 2.1: Cicli di σ

cicli e ciascuno viene mandato nel successivo da σ con l'eccezione dell'ultimo elemento prima della seconda parentesi che viene mandato nel primo (dopo la prima parentesi). Si noti che è indifferente da quale elemento si comincia a scrivere un ciclo, cosicché $(2, 5, 4) = (5, 4, 2) = (4, 2, 5)$, conta solo l'ordine (ciclico) in cui vengono rappresentati gli elementi che compaiono al suo interno. Inoltre la scrittura $\sigma = (1, 3)(2, 5, 4)$ può anche essere letta come una composizione ovvero σ è la permutazione che si ottiene componendo (non importa in che ordine) i suoi cicli. Nel caso in questione σ si ottiene componendo la permutazione individuata dal ciclo $(1, 3)$ con quella individuata dal ciclo $(2, 5, 4)$ o da quella individuata dal ciclo $(2, 5, 4)$ con quella individuata dal ciclo $(1, 3)$.

Questa descrizione informale può essere resa più rigorosa definendo una relazione di equivalenza in X: $i \sim j$ se e solo se esiste un intero k tale che $j = \sigma^k(i)$. Ogni classe di equivalenza di questa relazione sono i sottoinsiemi di X i cui elementi sono individuati dai cicli di σ. I cicli non sono altro che la restrizione di σ a queste classi di equivalenza (su ciascuna delle quali σ opera come una permutazione). La permutazione σ è in ogni caso uguale alla composizione, in qualsiasi ordine, dei suoi cicli.

La permutazione identica viene usualmente denotata con Id e tutti i suoi cicli contengono un solo elemento.

La notazione di σ come prodotto di cicli disgiunti viene detta *rappresentazione in forma ciclica* della permutazione σ.

2.1.1 Composizione di permutazioni in forma ciclica

Illustriamo con un esempio come effettuare la composizione di due (o più) permutazioni in forma ciclica. Partiamo da due permutazioni

$$\begin{aligned} \sigma &= (1,2,3)(4,5) \\ \tau &= (1,2,3,4)(6,7) \end{aligned}$$

definite sull'insieme $X = \{\, 1,2,3,4,5,6,7 \,\}$ e supponiamo di voler calcolare $\sigma \circ \tau$. Per comodità di notazione poniamo $\tau_1 = (1,2,3,4)$, $\tau_2 = (6,7)$, $\sigma_1 = (1,2,3)$ e $\sigma_2 = (4,5)$ Procediamo allora applicando di nell'ordine dapprima i cicli di τ e poi quelli di σ come segue:

- scegliamo un elemento di X, ad esempio 1: τ_1 manda 1 in 2, τ_2 fissa il 2, σ_1 manda il 2 in 3 e σ_2 fissa il 3. Pertanto 1 viene mandato in 3 da $\sigma \circ \tau$. Cominciamo a scrivere $(1,3\ldots$

- Riprendiamo dall'ultimo numero scritto: 3. τ_1 manda 3 in 4, τ_2 fissa il 4, σ_1 fissa il 4 e σ_2 manda il 4 in 5. Pertanto 3 viene mandato in 5 da $\sigma \circ \tau$. Aggiungiamo allora 5 alla scrittura precedente ottenendo $(1,3,5\ldots$

- Riprendiamo dall'ultimo numero scritto: 5. τ_1 fissa il 5, τ_2 fissa il 5, σ_1 fissa il 5 e σ_2 manda il 5 in 4. Pertanto 5 viene mandato in 4 da $\sigma \circ \tau$. Aggiungiamo allora 4 alla scrittura precedente ottenendo $(1,3,5,4\ldots$

- Riprendiamo dall'ultimo numero scritto: 4. τ_1 manda il 4 in 1, τ_2 fissa il 1, σ_1 manda 1 in 2 e σ_2 fissa il 2. Pertanto 4 viene mandato in 2 da $\sigma \circ \tau$. Aggiungiamo allora 2 alla scrittura precedente ottenendo $(1,3,5,4,2\ldots$

- Riprendiamo dall'ultimo numero scritto: 2. τ_1 manda il 2 in 3, τ_2 fissa il 3, σ_1 manda 3 in 1 e σ_2 fissa 1. Pertanto 4 viene mandato in 1 da $\sigma \circ \tau$: il ciclo si chiude. Aggiungiamo allora una parentesi chiusa alla scrittura precedente ottenendo $(1,3,5,4,2)$. Questo è uno dei cicli di $\sigma \circ \tau$.

- scegliamo un elemento di X che non compare tra quelli che abbiamo già scritto, ad esempio 6: τ_1 fissa il 6, τ_2 manda 6 in 7, σ_1 fissa il 7 e σ_2 fissa il 7. Pertanto 6 viene mandato in 7 da $\sigma \circ \tau$. Aggiungiamo il principio del secondo ciclo alla precedente scrittura $(1,3,5,4,2)(6,7\ldots$

- Riprendiamo dall'ultimo numero scritto: 7. τ_1 fissa il 7, τ_2 manda 7 in 6, σ_1 fissa il 6 e σ_2 fissa il 6. Pertanto 7 viene mandato in 6 da $\sigma \circ \tau$: il

ciclo si chiude. Aggiungiamo allora una parentesi chiusa alla scrittura precedente ottenendo $(1, 3, 5, 4, 2)(6, 7)$.

Dal momento che abbiamo considerato l'azione di $\sigma \circ \tau$ su tutti gli elementi di X il nostro calcolo è terminato e $(1, 3, 5, 4, 2)(6, 7)$ è la rappresentazione in forma ciclica di $\sigma \circ \tau$.

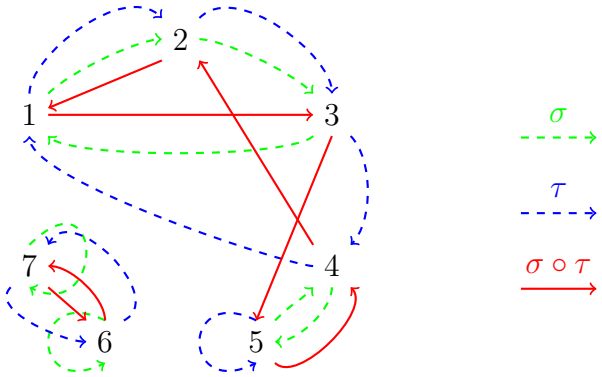


Figura 2.2: $\sigma \circ \tau$

Nella figura 2.2 si possono vedere i diagrammi a frecce in verde σ, in blu di τ ed in rosso di $\sigma \circ \tau$.

2.1.2 Permutazione inversa

Rovesciando le frecce nel diagramma a frecce di una permutazione si ottiene il diagramma della funzione inversa. Si veda ad esempio la figura 2.3 dove è rappresentata in tratteggiato la permutazione inversa di $\sigma = (1, 3)(2, 5, 4)$ su $X = \{ 1, 2, 3, 4, 5, 6 \}$.

La forma ciclica dell'inversa di una permutazione si ottiene quindi rovesciando l'ordine in cui sono scritti i vari elementi nei cicli. Ad esempio:

1. se $\sigma = (1, 3)(2, 5, 4)$ allora si ha $\sigma^{-1} = (1, 3)(2, 4, 5)$ (si noti che $(1, 3) = (3, 1)$),

2. se invece
$$\sigma = (1, 3, 8)(2, 5, 4, 9, 10)(11, 12, 43)$$
allora si tova
$$\sigma^{-1} = (1, 8, 3)(2, 10, 9, 4, 5)(11, 43, 12).$$

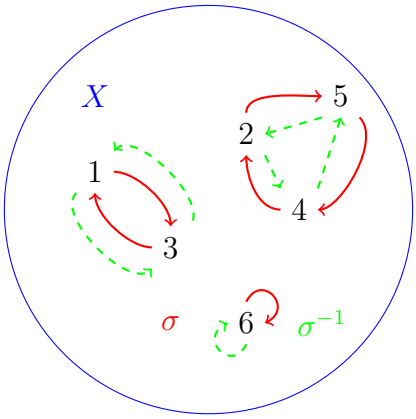


Figura 2.3: Cicli di σ^{-1}

2.1.3 Ordine o periodo di una permutazione.

In modo del tutto analogo al Lemma 1.14 si dimostra il seguente:

Lemma 2.1. *Per ogni permutazione σ su di un insieme finito X esiste un numero intero positivo t tale che $\sigma^t = \mathrm{Id}$.*

di conseguenza si può dare la seguente definizione

Definizione 2.2. Data una permutazione σ su di un insieme finito X si dice periodo o ordine di σ e si indica con $o(\sigma)$ o con $|\sigma|$ il più piccolo intero positivo t tale che $\sigma^t = \mathrm{Id}$.

Analogamente al caso delle classi di resto invertibili si dimostra la seguente proposizione.

Proposizione 2.3. *Se s è un intero positivo tale che $\sigma^s = \mathrm{Id}$ allora il periodo di σ divide s.*

Calcolo del periodo di una permutazione in forma ciclica

La lunghezza di un ciclo di una permutazione è il numero degli elementi elencati nel ciclo. Ad esempio, $(1, 3, 5)$ è un ciclo di lunghezza 3.

Lasciamo allo studente come esercizio quello di dimostrare che il periodo di una permutazione è il minimo comune multiplo delle lunghezze dei cicli della sua rappresentazione in forma ciclica.

Ad esempio:

1. $\sigma = (1, 3)(2, 5, 4)$ ha periodo 6.
2. $\sigma = (1, 3, 8)(2, 5, 4, 9, 10)(11, 12, 43)$ ha periodo 15.

2.2 Segno di una permutazione

Data una permutazione $\sigma \in S_n$ consideriamo la seguente espressione detta *segno della permutazione* σ:

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i} = \frac{\prod_{1 \le i < j \le n} (\sigma(j) - \sigma(i))}{\prod_{1 \le i < j \le n} (j - i)} \tag{2.1}$$

Poiché al variare di i e j in modo che $1 \le i < j \le n$ gli insiemi $I_{i,j} = \{ i, j \}$ costituiscono la totalità dei sottoinsiemi di $X = \{ 1, \ldots, n \}$ che hanno due elementi e siccome σ è una permutazione si trova che gli insiemi $\sigma(I_{i,j}) = \{ \sigma(i), \sigma(j) \}$ costituiscono anch'essi a totalità dei sottoinsiemi di X che hanno due elementi. Ne consegue che le differenze che compaiono al numeratore ed al denominatore dell'ultimo membro della (2.1) coincidono a meno del segno, essendo, a parte l'ordine con cui vengono eseguite, le differenze tra i due elementi di ciascuno dei sottoinsiemi di X con due elementi. Questo fatto ha come banale conseguenza che $\operatorname{sgn}(\sigma) = \pm 1$. Diremo allora che σ è pari se $\operatorname{sgn}(\sigma) = 1$ mentre σ viene detta permutazione dispari se $\operatorname{sgn}(\sigma) = -1$.

Lemma 2.4. *Per ogni permutazione $\tau \in S_n$ si ha*

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\tau(\sigma(j)) - \tau(\sigma(i))}{\tau(j) - \tau(i)} \tag{2.2}$$

Dimostrazione. Poiché σ è biunivoca, ogni sottoinsieme $I_{i,j} = \{ i, j \} \subseteq X$ con $i < j$, è della forma $\{ i, j \} = \sigma(I_{l,m}) = \{ \sigma(l), \sigma(m) \}$, per un unico sottoinsieme $I_{l,m}$ di X con $l < m$. In questo modo ad ogni sottoinsieme $\{ i, j \}$ (dove $i < j$) di X corrisponde il fattore $j - i$ al denominatore ed il fattore $\sigma(l) - \sigma(m) = \pm(j - i)$ al numeratore di (2.1). Notando che affermare che $\tau(i) - \tau(j)$ ha lo stesso segno di $i - j$ equivale ad affermare che $\tau(\sigma(l)) - \tau(\sigma(m))$ ha lo stesso segno di $\sigma(l) - \sigma(m) = \pm(j - i)$ si evince che nel passare dall'espressione (2.1) a (2.2) cambiano di segno lo stesso numero di fattori sia al numeratore che al denominatore. La tesi segue da fatto che entrambe queste espressioni hanno quindi lo stesso segno e sono entrambe uguali a ± 1. □

Proposizione 2.5. *Comunque scelte σ e τ in S_n si ha*

$$\operatorname{sgn}(\tau \circ \sigma) = \operatorname{sgn}(\tau) \operatorname{sgn}(\sigma).$$

Dimostrazione.

$$\begin{aligned}\operatorname{sgn}(\tau\circ\sigma) &= \prod_{1\le i<j\le n}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{j-i}\\ &= \prod_{1\le i<j\le n}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\tau(j)-\tau(i)}\prod_{1\le i<j\le n}\frac{\tau(j)-\tau(i)}{j-i}\\ &= \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)\end{aligned}$$

Dove nell'ultimo passaggio si è fatto uso del Lemma 2.4. □

Un ciclo $\tau = (a, b)$ di lunghezza due viene detto scambio. Supponiamo che $a < b$ e calcoliamo il segno di τ con la formula 2.1. Se i e j sono entrambi diversi da a e b allora $\frac{\tau(j)-\tau(i)}{j-i} = \frac{j-i}{j-i} = 1$. Poi vi sono i termini in cui uno uno solo degli indici è diverso da a o b. Questi a loro volta si dividono in tre gruppi:

1. $i < a$; fattori della forma $\frac{\tau(a)-\tau(i)}{a-i} = \frac{b-i}{a-i}$ e della forma $\frac{\tau(b)-\tau(i)}{b-i} = \frac{a-i}{b-i}$ il cui prodotto è uguale a 1,
2. $a < i < b$; fattori della forma $\frac{\tau(i)-\tau(a)}{i-a} = \frac{i-b}{i-a}$ e della forma $\frac{\tau(b)-\tau(i)}{b-i} = \frac{a-i}{b-i}$ il cui prodotto è ancora uguale a 1,
3. $b < i$; fattori della forma $\frac{\tau(i)-\tau(a)}{i-a} = \frac{i-b}{i-a}$ e della forma $\frac{\tau(i)-\tau(b)}{i-b} = \frac{i-a}{i-b}$ il cui prodotto è ancora uguale a 1,
4. Il fattore $\frac{\tau(b)-\tau(a)}{b-a} = \frac{a-b}{b-a} = -1$.

Ne consegue che $\operatorname{sgn}(\tau) = -1$. Ovvero *uno scambio è una permutazione dispari*.

Notando che un ciclo $(a_1, \ldots, a_k)$ di lunghezza k può essere scritto come prodotto di $k-1$ scambi: $(a_1, \ldots, a_k) = (a_{k-1}, a_k) \circ (a_{k-2}, a_k) \circ \cdots \circ (a_2, a_k) \circ (a_1, a_k)$, dalla Proposizione 2.5 si trovano il seguenti Corollari.

Corollario 2.6. *Il segno di un ciclo di lunghezza k è $(-1)^{k-1}$.*

Corollario 2.7. *Il segno di una permutazione σ è $(-1)^t$ dove t è il numero dei cicli di lunghezza pari della rappresentazione in forma ciclica di σ.*

Definizione 2.8. Il sottoinsieme di S_n i cui elementi sono permutazioni pari viene denotato con A_n e viene detto insieme alternante su n simboli.

2.2.1 Esercizi:

Esercizio 2.1. Scrivere in forma ciclica tutti gli elementi di A_3 ed A_4.

Esercizio 2.2. Dimostrare che se $n \geq 2$ allora $|S_n| = 2|A_n|$, ovvero che in S_n il numero delle permutazioni pari eguaglia il numero delle permutazioni dispari. In particolare $|A_n| = \frac{n!}{2}$. *Sugg: si ponga* $P = A_n$ *e* $D = S_n \setminus A_s$, $\tau = (1, 2)$*; mostrare che la funzione* $f \colon P \to D$ *definita da* $f(\sigma) = \tau \circ \sigma$ *è biunivoca.*

Capitolo 3

Gruppi

3.1 I gruppi

3.1.1 Operazioni su di un insieme

Un'operazione (binaria) su di un insieme A è una funzione $f\colon A \times A \to A$. Per comodità e tradizione di notazione si usa scrivere $a \cdot b$ al posto di si $f(a, b)$. In questo caso diremo che il simbolo $\cdot$ è una operazione su A. La scelta del simbolo $\cdot$ è dovuta alla tradizione, nulla vieta di usare simboli come $\oplus$, $\diamond$, $+$, ecc.... Scriveremo spesso ab per indicare $a \cdot b$ sottointendendo il simbolo di operazione. Con la scrittura $(ab)c$ intenderemo allora $(a \cdot b) \cdot c = f(f(a, b), c)$.

Un'operazione su di un insieme A è detta

1. essere *associativa* se per ogni a, b e $c \in A$ vale l'uguaglianza

$$(ab)c = a(bc);$$

2. ammettere *elemento neutro* se esiste un elemento in A, denotato usualmente con 1, tale che per ogni $a \in A$ si abbia

$$a \cdot 1 = 1 \cdot a = a.$$

3. essere *commutativa* se per ogni a, $b \in A$ vale l'uguaglianza

$$ab = ba;$$

Se l'operazione $\cdot$ ammette un elemento neutro, un elemento $a \in A$ è detto essere *invertibile* (rispetto all'operazione $\cdot$) se esiste un altro elemento in A, usualmente denotato con a^{-1} tale che $a^{-1}a = aa^{-1} = 1$.

3.1.2 Gruppi: definizione ed esempi

Definizione 3.1. Un gruppo $(G, \cdot)$ è una coppia composta da un insieme G ed un'operazione $\cdot$ su G che risulti essere associativa, ammetta un elemento neutro e rispetto alla quale ogni elemento di G risulti invertibile.

Un gruppo la cui operazione sia commutativa è detto gruppo abeliano. In tal caso spesso (ma non obbligatoriamente) si usa il simbolo $+$ (al posto di $\cdot$) per indicare l'operazione in esso definita, il simbolo 0 (zero) per denotare l'elemento neutro di $+$, ed il simbolo $-g$ per indicare l'inverso di un elemento $g \in G$ rispetto a tale operazione. In tal caso l'elemento $-g$, che è l'inverso di g rispetto all'operazione $+$, viene anche detto *opposto* di g.

Esempi

- **Il gruppo** $(\mathbb{Z}, +)$. L'insieme dei numeri interi è un gruppo abeliano infinito rispetto all'operazione di somma di numeri interi. Tale operazione è infatti notoriamente associativa, ammette lo 0 come elemento neutro e ogni elemento ammetto un elemento opposto (inverso rispetto alla somma).

- **Il gruppo** $(\mathbb{R}^*, \cdot)$ L'insieme dei numeri reali non nulli è chiaramente un gruppo abeliano infinito rispetto all'operazione di prodotto di numeri reali.

- $(\mathbb{Z}^*, \cdot)$ non è un gruppo. Infatti, pur essendo il prodotto di numeri interi non nulli un'operazione associativa in $\mathbb{Z}^*$ con elemento neutro (1), l'elemento 2 non ha alcun inverso in $\mathbb{Z}$ rispetto al prodotto.

- $(\mathbb{R}, \cdot)$ non è un gruppo. Infatti, pur essendo il prodotto di numeri reali un'operazione associativa in $\mathbb{R}$ con elemento neutro (1), l'elemento 0 non ha alcun inverso in $\mathbb{Z}$ rispetto al prodotto.

- Il gruppo $(S_n, \circ)$. Le permutazioni su un insieme con n elementi formano un gruppo finito, **non abeliano se** $n > 2$, rispetto alla composizione. L'elemento neutro è la permutazione identica. L'inverso di una permutazione è la sua permutazione inversa.

- Il gruppo $(\mathbb{Z}_n, +)$. Le classi di resto modulo n formano un gruppo abeliano finito rispetto alla somma di classi di resto. L'elemento neutro è la classe di 0, l'opposto di una classe è la classe opposta.

- Il gruppo $(G(n), \cdot)$. Le classi di resto invertibili modulo n formano un gruppo abeliano finito rispetto al prodotto di classi di resto. L'elemento neutro è la classe di 1, l'inverso di una classe è la classe inversa.

- Il gruppo $(\mathrm{GL}(2,\mathbb{R}),\cdot)$. L'insieme delle matrici 2×2 a coefficienti reali $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ con $ad-bc\neq 0$ formano un gruppo non abeliano infinito rispetto al prodotto di matrici (esercizio).

3.1.3 Tavola di moltiplicazione di un gruppo ed isomorfismo tra gruppi

La tavola di moltiplicazione $\mathfrak{T}$ di un gruppo finito G è una tabella in cui righe e colonne sono indicizzate dagli elementi del gruppo G. Se g ed h sono due elementi di G che indicizzano rispettivamente una riga ed una colonna di $\mathfrak{T}$ allora nella casella ottenuta incrociando dette riga e colonna comparirà l'elemento gh.

Costruiamo subito come esempio la tavola di moltiplicazione del gruppo $S_3 = \{\,\mathrm{Id}, (1,2,3), (1,3,2), (1,2), (1,3), (2,3)\,\}$ (dove l'operazione sottintesa è quella di composizione). Nelle tabelle successive la prima riga e la prima colonna che sono separate da una doppia linea, fungono da segnaposti per gli indici e non fanno propriamente parte delle tavole di moltiplicazione.

S_3	Id	$(1,2,3)$	$(1,3,2)$	$(1,2)$	$(1,3)$	$(2,3)$
Id	Id	$(1,2,3)$	$(1,3,2)$	$(1,2)$	$(1,3)$	$(2,3)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	Id	$(1,3)$	$(2,3)$	$(1,2)$
$(1,3,2)$	$(1,3,2)$	Id	$(1,2,3)$	$(2,3)$	$(1,2)$	$(1,3)$
$(1,2)$	$(1,2)$	$(2,3)$	$(1,3)$	Id	$(1,3,2)$	$(1,2,3)$
$(1,3)$	$(1,3)$	$(1,2)$	$(2,3)$	$(1,2,3)$	Id	$(1,3,2)$
$(2,3)$	$(2,3)$	$(1,3)$	$(1,2)$	$(1,3,2)$	$(1,2,3)$	Id

Ecco la tavola di moltiplicazione si Z_4 dove per brevità scriveremo un intero a al posto della classe di resto $[a]_4$:

$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Ed ora la tavola di moltiplicazione si $G(5)$. Anche qui per brevità scriveremo un intero a al posto della classe di resto $[a]_5$

$G(5)$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Notiamo che rimpiazzando nella tavola di moltiplicazione di $G(5)$ il simbolo 1 con 0, 2 con 1, 4 con 2 e 3 con 3 si ottiene la tavola di moltiplicazione di $\mathbb{Z}_4$: abbiamo appena scoperto il concetto di *isomorfismo tra gruppi*. Due gruppi $(G, \cdot)$ e $(G', \cdot)$ si dicono isomorfi se hanno la stessa tavola di moltiplicazione. In maniera equivalente ma più rigorosa si dice che $(G, \cdot)$ e $(G', \cdot)$ sono tra loro isomorfi se esiste una funzione biunivoca $f\colon G \to G'$ tale che, comunque scelti a e b appartenenti a G, si abbia $f(a \cdot b) = f(a) \cdot f(b)$.

3.1.4 Unicità di elemento neutro ed inverso

Vediamo alcuni lemmi tecnici che ci serviranno in in seguito.

Lemma 3.2. *In un gruppo G ogni elemento ha un unico inverso.*

Dimostrazione. Sia $g \in G$ e si supponga che esistano $h, k \in G$ tali che $gh = hg = gk = kg = 1$. allora $h = h \cdot 1 = h(gk) = (hg)k = 1 \cdot k = k$. □

Lemma 3.3. *Se g ed h sono due elementi di un gruppo G tali che $hg = g$ allora $h = 1$. In particolare esiste un solo elemento neutro in G.*

Dimostrazione. $h = h(gg^{-1}) = (hg)g^{-1} = gg^{-1} = 1$. Se esistessero due elementi neutri 1 ed e avremmo $1e = 1$ e pertanto per quanto appena dimostrato (caso in cui $g = 1$ e $h = e$) si ha $e = 1$. □

3.2 Sottogruppi

Consideriamo l'insieme A_n delle permutazioni pari su n elementi. Rispetto alla composizione di permutazioni questo insieme risulta essere un gruppo. Sappiamo infatti che la composizione di permutazioni è un'operazione associativa, la composizione di due permutazioni pari è una permutazione pari e l'inversa di una permutazione pari è anch'essa pari. Quindi A_n è un sottoinsieme di S_n che risulta essere un gruppo rispetto alla stessa operazione definita in S_n. Diremo allora che A_n è un *sottogruppo* di S_n.

Definizione 3.4. Un sottoinsieme non vuoto $H \subseteq G$ di un gruppo $(G, \cdot)$ è detto sottogruppo di G se, comunque scelti $a, b \in H$, il prodotto $a \cdot b^{-1}$ appartiene ancora ad H. In tal caso scriveremo $H \leq G$ per indicare che H è un sottogruppo di G.

Supponiamo ora che H sia un sottogruppo di un gruppo G (secondo la definizione appena data). Poiché H non è vuoto, esiste un elemento $h \in H$ e pertanto l'elemento neutro 1_G di G appartiene ad H, infatti $1_G = hh^{-1} \in H$. Inoltre se $a \in H$ allora, in base alla definizione di sottogruppo, $a^{-1} = 1_G a^{-1} \in H$. Pertanto

1. comunque scelti due elementi $a, b \in H$ il prodotto $ab = a(b^{-1})^{-1} \in H$ H contiene i prodotti delle coppie di suoi elementi,

2. ogni elemento di H ha inverso in H.

3. l'elemento neutro di G appartiene ad H

4. H risulta essere un gruppo rispetto all'operazione definita in G.

Viceversa è facile vedere che, se un sottoinsieme non voto $H \subseteq G$ risulta essere un gruppo rispetto all'operazione definita in G, allora H è un sottogruppo di G nel senso della Definizione 3.4. La dimostrazione di questo asserto è lasciata per esercizio (si devono usare i Lemmi del paragrafo 3.1.4).

L'insieme composto dal solo elemento neutro di un gruppo G è un sottogruppo di G detto sottogruppo banale o identico. Il gruppo G è sempre un sottogruppo di sé stesso.

Esercizio 3.1. Dimostrare che l'intersezione $I = H \cap K$ di due sottogruppi H e K di un gruppo G è un sottogruppo di G di H e K.

Esercizio 3.2. Dimostrare che l'unione $I = H \cup K$ di due sottogruppi H e K di un gruppo G è un sottogruppo di G solo se $H \subseteq K$ o $K \subseteq H$..

3.2.1 Sottogruppi di $\mathbb{Z}$

È facile vedere che i numeri interi pari formano un sottogruppo del gruppo $(\mathbb{Z}, +)$, lo stesso dicasi per l'insieme dei numeri interi divisibili per 3. Più in generale L'insieme $n\mathbb{Z} := \{\, nh \mid h \in \mathbb{Z} \,\}$, i cui elementi sono i numeri interi multipli di n, è un sottogruppo di $\mathbb{Z}$ (dove, come faremo anche in seguito, sottintendiamo l'operazione di somma). Infatti $n\mathbb{Z}$ è non vuoto e comunque scelti nh ed nk in $n\mathbb{Z}$ si ha $nh + (-nk) = n(h - k) \in n\mathbb{Z}$. Il sottogruppo banale di $\mathbb{Z}$ è anch'esso della forma $n\mathbb{Z}$ dove $n = 0$.

Cerchiamo ora di determinare tutti i sottogruppi del gruppo $\mathbb{Z}$. a tal scopo sarà utile il seguente risultato.

Lemma 3.5. *Se $0 < a < b$ sono due elementi positivi di un sottogruppo H di $\mathbb{Z}$ ed a non divide b, allora H contiene un numero intero positivo r strettamente minore di a.*

Dimostrazione. Siano q ed r il quoziente ed il resto della divisione di b per a. Avremo $b = aq + r$. Dal momento che a non divide b il resto r sarà diverso da zero pertanto $0 < r < a$. Inoltre $r = b - aq$. Poiché $a \in H$ anche $aq \in H$ cosicché r si ottiene sommando all'elemento b di H l'opposto dell'elemento aq di H. Dalla definizione di sottogruppo si trova allora che $r \in H$. □

Teorema 3.6. *Se H è un sottogruppo di Z allora esiste un unico intero non negativo n, detto generatore di H, tale che $H = n\mathbb{Z}$.*

Dimostrazione. L'unicità di n viene dal fatto che se $n = 0$ se e solo se $H = \{ 0 \}$, altrimenti n deve essere il più piccolo elemento positivo di H.

Mostriamo ora l'esistenza di n. Se $H = \{ 0 \}$ allora basta scegliere $n = 0$. Altrimenti esiste in H un elemento $t \neq 0$. Poiché anche $-t$ appartiene ad H ed uno tra t e $-t$ è un numero positivo, possiamo anche supporre che H contenga almeno un numero positivo. Chiamiamo n il più piccolo intero positivo contenuto in H. Se k è un elemento non nullo di H allora uno tra k o $-k$ è un numero positivo, che chiamiamo s, in H. Dal Lemma 3.5 e dalla scelta fatta dell'elemento n troviamo di nuovo che n divide s (altrimenti ci sarebbe in H un elemento positivo più piccolo di n). Pertanto n divide s, ovvero n divide k di modo che $k = nh \in nZ$. Questo mostra che $H \subseteq n\mathbb{Z}$.Viceversa poiché $n \in H$ ogni multiplo di n è contenuto in H e pertanto $n\mathbb{Z} \leq H$. Visto che abbiamo ottenuto le due inclusioni $H \subseteq n\mathbb{Z}$ e $n\mathbb{Z} \leq H$ possiamo concludere che $H = n\mathbb{Z}$. □

Esercizio 3.3. Determinare il generatore di $n\mathbb{Z} \cap m\mathbb{Z}$ (che è un sottogruppo di $\mathbb{Z}$ in base all'Esercizio 3.1).

3.2.2 Laterali di un sottogruppo

Riprendiamo in esame la costruzione delle classi di resto modulo n. Queste sono le classi di equivalenza della relazione definita in $\mathbb{Z}$ da $x \equiv y$ se e solo se $x + (-y) \in n\mathbb{Z}$. Gli ingredienti di questa definizione hanno un aspetto di natura gruppale. Infatti questa relazione diventa un caso particolare della seguente: *dati un gruppo G ed un suo sottogruppo H possiamo definire in G una relazione $\sim_d$ (rispettivamente $\sim_s$) in G dicendo che due elementi x ed y di G sono in relazione destra $x \sim_d y$ (risp. sinistra $x \sim_s y$) se e solo se $xy^{-1} \in H$ (risp. $x^{-1}y \in H$).* Le relazioni appena definite sono di equivalenza, lo mostriamo per la relazione $\sim_d$ e lasciamo al lettore il compito di verificarlo per la relazione $\sim_s$.

- Proprietà riflessiva. Comunque scelto $g \in G$ si ha $gg^{-1} = 1 \in H$, cosicché $g \sim_d g$.

- Proprietà simmetrica. Comunque scelti g e g' in G tali che $g \sim_d g'$ si ha $h = gg'^{-1} \in H$. Poiché H contiene l'inverso di ciascun suo elemento troviamo $h^{-1} = g'g^{-1} \in H$ e pertanto $g' \sim_d g$.

- Proprietà transitiva. Se $g, l, m \in G$ sono tre elementi tali che $g \sim_d l$ e $l \sim_d m$ allora $h = gl^{-1}$ ed $h' = lm^{-1}$ sono due elementi di H. Poiché

H contiene i prodotti delle coppie dei suoi elementi si ha $gm^{-1} = g(l^{-1}l)m^{-1} = (gl^{-1})(lm^{-1}) = hh' \in H$. Ne consegue che $g \sim_d m$.

Le classi di equivalenza della relazione $\sim_d$ (rispettivamente $\sim_s$) sono detti laterali destri (risp. sinistri) di H in G.

Cerchiamo ora di determinare il laterale destro di H in G che ha come rappresentante un elemento $x \in G$. La classe di equivalenza $[x]$ dell'elemento x è il sottoinsieme di G formato da tutti gli elementi di G che sono in relazione con x. Notiamo che un elemento $g \in G$ è in relazione con x se e solo se esiste un elemento $h = gx^{-1} \in H$ tale che $g = hx$. Possiamo allora scrivere $[x] = \{\, g \in G \mid g \sim_d x \,\} = \{\, hx \mid h \in H \,\}$, in particolare il laterale destro di H in G avente x come rappresentante è composto da tutti gli elementi di G che si ottengono moltiplicando a destra x per ciascun elemento di H. La notazione più naturale per indicare il laterale destro di H in G individuato da x è quindi $Hx := \{\, hx \mid h \in H \,\}$. Il laterale sinistro di H in G individuato da x si verifica facilmente essere l'insieme $xH := \{\, xh \mid h \in H \,\}$. Notiamo infine che dovendo ogni elemento x appartenere alla propria classe di equivalenza si ha $x \in Hx$ (risp. $x \in xH$).

Esempi

Determiniamo i laterali destri e sinistri di $H = \{\, \mathrm{Id}, (1,2) \,\}$ in S_3.

LATERALI SINISTRI

- $H\mathrm{Id} = \{\, \mathrm{Id} \circ \mathrm{Id}, (1,2) \circ \mathrm{Id} \,\} = H$,
- $H(1,3) = \{\, \mathrm{Id} \circ (1,3), (1,2) \circ (1,3) \,\} = \{\, (1,3), (1,3,2) \,\}$,
- $H(2,3) = \{\, \mathrm{Id} \circ (2,3), (1,2) \circ (2,3) \,\} = \{\, (2,3), (1,2,3) \,\}$.

LATERALI DESTRI

- $\mathrm{Id}H = \{\, \mathrm{Id} \circ \mathrm{Id}, \mathrm{Id} \circ (1,2) \,\} = H$,
- $(1,3)H = \{\, (1,3) \circ \mathrm{Id}, (1,3) \circ (1,2) \,\} = \{\, (1,3), (1,2,3) \,\}$,
- $(2,3)H = \{\, (2,3) \circ \mathrm{Id}, (2,3) \circ (1,2) \,\} = \{\, (2,3), (1,3,2) \,\}$,

Si noti che esistono degli elementi $x \in S_3$ tali che $xH \neq Hx$.

I laterali destri $n\mathbb{Z} + x$ del sottogruppo $n\mathbb{Z}$ in $\mathbb{Z}$ sono le classi di resto modulo n. Lo stesso dicasi per i laterali sinistri (questo dipende dal fatto che $\mathbb{Z}$ è un gruppo abeliano). In questo caso per ogni $x \in \mathbb{Z}$ si ha $x + \mathbb{Z} = \mathbb{Z} + x$.

Un esempio più geometrico è il seguente: $G = \mathbb{R}^2 = \{\, (a,b) \mid a, b \in \mathbb{R} \,\}$ è un gruppo rispetto alla somma di vettori $((a,b)+(c,d) = (a+c, b+d))$ ed $H = \{\, (x,0) \mid x \in \mathbb{R} \,\}$ (asse delle ascisse) è un sottogruppo di G. I laterali (destri o sinistri) di H in G sono le rette parallele all'asse delle ascisse (perché?).

3.2.3 Teorema di Lagrange

Una proprietà importante dei laterali di un sottogruppo, che è evidente anche negli esempi presentati, è che un qualsiasi laterale destro Hx (o sinistro xH) di un sottogruppo H in un gruppo G ha la stessa cardinalità di H come risulta dal seguente lemma.

Lemma 3.7. *Per ogni laterale Hx (risp. xH) di un sottogruppo H in un gruppo G esiste una funzione biunivoca $f\colon H \to Hx$ (risp $f\colon H \to xH$). In particolare se H è un insieme finito si ha che $|H| = |Hx| = |xH|$ per ogni $x \in G$*

Dimostrazione. Si definisca $f(h) = xh$. Per come è stato definito $Hx = \{\, hx \mid h \in H \,\} = \{\, f(h) \mid h \in H \,\} = f(H)$, la funzione f risulta banalmente essere suriettiva. Mostriamo che f è anche iniettiva. Supponiamo che $f(h) = f(h')$ dove h ed h' sono due elementi di H. Allora $h = h(xx^{-1}) = (hx)x^{-1} = f(h)x^{-1} = f(h')x^{-1} = (h'x)x^{-1} = h'(xx^{-1}) = h'$. □

Come corollario si ha il seguente celebre risultato.

Teorema 3.8 (di Lagrange)**.** *Se G è un gruppo finito ed H un suo sottogruppo allora $|G| = r|H|$ dove r è il numero dei laterali destri o sinistri di H in G.*

Dimostrazione. Indichiamo con r_d il numero dei laterali sinistri di H in G e poniamo $n = |H|$. Poiché $\sim_d$ è una relazione di equivalenza, i laterali destri di H in G formano una partizione in r_d sottoinsiemi disgiunti ciascuno dei quali, per il Lemma 3.7, contiene lo stesso numero n di elementi. Ne consegue che G contiene esattamente $nr_d = |G|$ elementi.

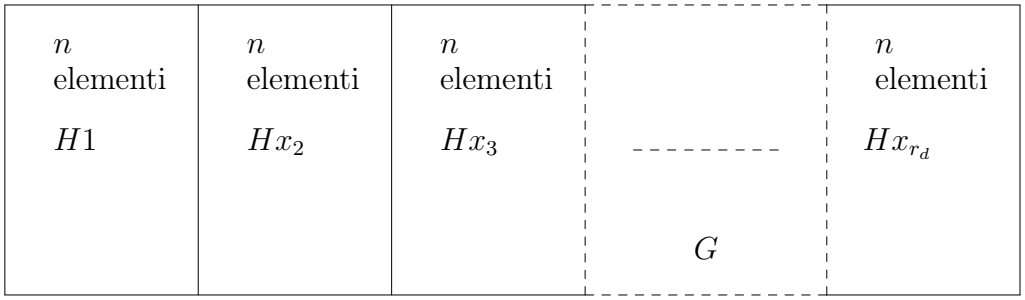


Figura 3.1: Partizione indotta dai laterali

Ragionando in modo del tutto analogo sui laterali sinistri e ponendo r_s uguale al loro numero si ottiene $r_s n = |G|$, da cui si ricava $r_s = r_d = r$. □

3.2.4 Periodo di un elemento e gruppi ciclici

Dato un elemento g in gruppo G ed un numero intero m si definisce

$$g^m = \begin{cases} \underbrace{g \cdots g}_{m \text{ volte}} & \text{se } m > 0, \\ \underbrace{g^{-1} \cdots g^{-1}}_{-m \text{ volte}} & \text{se } m < 0, \\ 1 & \text{se } m = 0. \end{cases}$$

Valgono allora le regole delle potenze: per ogni coppia di numeri interi n ed m si ha $g^{n+m} = g^n g^m$ e $(g^n)^m = g^{nm}$.

Nel caso in cui si adotti una notazione additiva per l'operazione del gruppo G si parlerà di multipli invece che di potenze e scriveremo mg invece di g^m. Le regole delle potenze diventano in questo caso: per ogni coppia di numeri interi n ed m si ha $(n+m)g = ng + mg$ e $(nm)g = n(mg)$.

Un elemento g di un gruppo G viene detto periodico, o di periodo finito, se esiste un intero positivo t tale che $g^t = 1$, altrimenti g viene detto elemento di periodo infinito. Analogamente a quanto visto per le permutazioni si definisce *periodo o ordine* di un elemento periodico g il numero intero positivo

$$\min \left\{ t \in \mathbb{Z}^+ \mid g^t = 1 \right\}.$$

Il periodo di g viene usualmente denotato con $|g|$ o con $o(g)$.

Lemma 3.9. *Siano G un gruppo e g un suo elemento periodico di periodo n. Allora, dati due interi h e k, si ha $g^h = g^k$ se e solo se $h \equiv k \bmod n$.*

Dimostrazione. Possiamo supporre $h < k$ senza perdere di generalità (perché?). Poniamo $s = k - h > 0$. Troviamo $g^s = g^{k-h} = g^k (g^h)^{-1} = g^h (g^h)^{-1} = 1$. Sia $r = s - qn$ è il resto della divisione di s per n. Supponiamo per assurdo che r sia non nullo. In tal caso avremo $0 < r < n$. e $g^r = g^{s-qn} = g^s (g^n)^q = 1 \cdot 1^q = 1$ che va contro contro l'aver scelto n uguale al periodo di g. Pertanto $r = 0$ ed n divide $s = k - h$. □

Definizione 3.10. Sia G un gruppo ed x un suo elemento. Si definisce sottogruppo ciclico di G generato da x l'insieme $\{ x^m \mid m \in \mathbb{Z} \}$ di tutte le potenze di x. Tale insieme viene denotato con $\langle x \rangle$ ed è un sottogruppo di G (come si vede subito dalla definizione di sottogruppo). Un gruppo G è detto ciclico se esiste un elemento $x \in G$ tale che $G = \langle x \rangle$.

Teorema 3.11. *Sia g un elemento di periodo finito n di un gruppo G allora la funzione $f \colon \mathbb{Z}_n \to \langle x \rangle$ definita da $f([m]_n) = x^m$ è ben definita e biunivoca. Inoltre $f([l]_n + [m]_n) = f([l]_n) \cdot f([m]_n)$ e pertanto f è un isomorfismo. In particolare $\langle x \rangle$ ha cardinalità uguale a al al periodo di x.*

Dimostrazione. Se $[m]_n = [m']_n$ allora $m \equiv m' \bmod n$, quindi, per il Lemma 3.9, $x^m = x^n$ e pertanto f è ben definita e non dipende dal rappresentante scelto per la classe di resto $[m]_n$. Per lo stesso lemma si ha che $f([m]_n) = f([m']_n)$ se e solo se $[m]_n = [m']_n$. Pertanto f è biunivoca. Infine si ha $f([l]_n + [m]_n) = f([l+m]_n) = x^{l+m} = x^l x^m = f([l]_n) \cdot f([m]_n)$. □

Esercizio 3.4. Dimostrare che se $g \in G$ è un elemento di periodo finito n e d è un divisore di n allora $\langle x \rangle$ ha un solo sottogruppo H di ordine d e che $H = \langle x^{\frac{n}{d}} \rangle$.

Corollario 3.12. *Un gruppo finito G di ordine p primo è necessariamente ciclico.*

Dimostrazione. Poiché $p > 1$ in G vi è almeno un elemento $g \neq 1$. Consideriamo il sottogruppo $H = \langle x \rangle$. Dal Teorema 3.11 sappiamo che la cardinalità di H è uguale a al periodo n di x. Dal teorema di Lagrange otteniamo che $n > 1$ è un divisore del numero primo p. Ne deduciamo che $n = p$ e che $G = H = \langle x \rangle$. □

3.3 Azioni di un gruppo su di un insieme

La geometria moderna studia gli invarianti sotto alcuni gruppi di trasformazioni. Ad esempio, le proprietà che accomunano tutti i triangoli sono quelle che sono invarianti sotto l'azione del gruppo delle affinità piane, la lunghezza di un segmento è un invariante sotto l'azione del gruppo delle isometrie, il numero degli elementi di un sottoinsieme di un insieme finito è invariante sotto il gruppo delle permutazioni di quell'insieme. Vogliamo formalizzare quindi il concetto di un gruppo che agisce su di un insieme.

Definizione 3.13. Un'azione (sinistra) di un gruppo G su di un insieme X è una funzione $G \times X \to X$ che manda la coppia (g, x) in un elemento di X denotato con $g \cdot x$ o, in breve, con gx, per la quale valgano le due seguenti proprietà:

(i) comunque scelto $x \in X$ si ha $1 \cdot x = x$,

(ii) comunque scelti $x \in X$ e $g, h \in G$ vale $g(hx) = (gh)x$.

Se un gruppo G ha un'azione su di un insieme X diremo che X è un G-insieme.

Facciamo alcuni esempi:

- $G = S_n$, $X = \{1, \ldots, n\}$. Per $\sigma \in S_n$ e $x \in X$ si pone $\sigma \cdot i = \sigma(i)$. Questa è un'azione di G su X, infatti per ogni $\sigma, \tau \in S_n$ e per ogni $x \in X$, si ha $1 \cdot x = \mathrm{Id}(x) = x$ e $\sigma \cdot (\tau \cdot x) = \sigma(\tau(x)) = (\sigma \circ \tau)(x) = (\sigma\tau) \cdot x$.

- $G = S_n$, $X = \mathcal{P}\{1, \ldots, n\}$ (insieme delle parti di $\{1, \ldots, n\}$). Per $\sigma \in S_n$ e $A = \{i_1, \ldots, i_k\} \in X$ si pone $\sigma A = \{\sigma(i_1), \ldots, \sigma(i_k)\} = \sigma(A)$.

- $M \in G = \mathrm{GL}(n, \mathbb{R})$ e $\vec{v} \in X = \mathbb{R}^n$ ($\vec{v}$ vettore colonna). Si pone $M \cdot \vec{v} = M\vec{v}$.

Se X è un G-insieme possiamo definire una relazione di equivalenza in X ponendo $x \sim y$ se e solo esiste $g \in G$ tale che $y = gx$. Valgono infatti le tre proprietà che caratterizzano le relazioni di equivalenza.

Riflessiva: Per ogni $x \in X$ si ha $x \sim x$ infatti $x = 1 \cdot x$.

Simmetrica: Si supponga che $x, y \in X$ siano tali che $x \sim y$, allora esiste $g \in G$ tale che $y = gx$ da cui $x = 1 \cdot x = (g^{-1}g)x = g^{-1}(gx) = g^{-1}y$ e pertanto $y \sim x$.

Transitiva: Si supponga che $x, y, z \in X$ siano tali che $x \sim y$ e $y \sim z$, allora esistono $g, h \in G$ tali che $y = gx$ e $z = hy$. Ne consegue che $z = hy = h(gx) = (hg)x$ e quindi $x \sim z$.

Definizione 3.14. Le classi di equivalenza della relazione descritta sopra sono dette *orbite* dell'azione di G su X, o, più brevemente, orbite di G su X se non vi può essere confusione sull'azione considerata di G su X.

Se X è un G-insieme e $x \in X$ allora l'orbita di x sotto l'azione di G è l'orbita che contiene x e viene indicata con $Gx = \{gx \mid g \in G\}$. Lo *stabilizzante* G_x di x in G è definito come $G_x = \{g \in G \mid gx = x\}$. Lo stabilizzante di x in G è un sottogruppo di G (esercizio). In modo analogo, per ogni $g \in G$, si può definire il sottoinsieme $\mathrm{Fix}(g) \subseteq X$ ponendo $\mathrm{Fix}(g) = \{x \in X \mid gx = x\}$.

Denotiamo con S l'insieme dei laterali sinistri di G_x in G e definiamo una funzione $f \colon S \to Gx$ come ponendo $f(gG_x) = gx$. Lasciamo al lettore il compito di verificare che questa funzione è ben definita e non dipende dal rappresentante g laterale gG_x, bensì dal laterale gG_x.

Teorema 3.15 (dell'orbita)**.** *La funzione f definita sopra è biunivoca e pertanto l'orbita dell'elemento x è in corrispondenza biunivoca con l'insieme dei laterali sinistri di G_x in G. In particolare se G ha ordine finito dal Teorema di Lagrange si trova $|Gx| = |G|/|G_x|$.*

Dimostrazione. Consideriamo un generico elemento $gx \in Gx$ avremo $gx = f(gG_x) \in f(S)$ cosicché f risulta essere suriettiva.

Se supponiamo che $f(gG_x) = f(g'G_x)$ allora $gx = g'x$ di modo che $x = x(g^{-1}g')$. Ne consegue che $g^{-1}g$ fissa x e quindi che $g^{-1}g \in G_x$. Quest'ultima affermazione è equivalente ad asserire che $gG_x = g'G_x$ e pertanto f risulta essere anche una funzione iniettiva. □

Teorema 3.16 (Fromula di Burnside)**.** *Il numero t delle orbite di un gruppo finito G su di un insieme finito X è uguale a*

$$t = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}(g).$$

Dimostrazione. Si consideri l'insieme il sottoinsieme S del prodotto cartesiano $G \times X$ definito da $S = \{\, (g, x) \in G \times X \mid gx = x \,\}$. Avremo allora $|S| = \sum_{g \in G} \mathrm{Fix}(g)$. Siano $x_1, \ldots, x_t$ un sistema di rappresentanti delle orbite $Gx_1, \ldots, Gx_t$. Per il teorema precedente e per il gatto che vale $x \in Gx_i$ se e solo se $Gx = Gx_i$, si ha anche $|S| = \sum_{x \in X} C_G(x) = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \sum_{x \in X} \frac{1}{|Gx|} = |G| \sum_{i=1}^{t} \sum_{x \in Gx_i} \frac{1}{|Gx|} = |G| \sum_{i=1}^{t} \sum_{x \in Gx_i} \frac{1}{|Gx_i|} = |G| \sum_{i=1}^{t} 1 = |G|t$. Eguagliando le due diverse epressioni ottenute per la cardinalità di S, si trova il nostro asserto. □

Mostriamo con un esempio come applicare la formula di Burnside a problemi di conteggio. Supponiamo di voler contare quante collane, distinte a meno di isometrie, si possono costruire con 4 perline gialle, 3 rosse e 3 blu. Possiamo pensare di colorare i vertici di un decagono regolare: 4 di giallo, 3 di rosso e 3 di blu. Il numero totale di collane che si possono disegnare si ottiene contando gli elementi dell'unica orbita del gruppo S_{10} sui vertici del decagono. Per fare questo utilizziamo il teorema dell'orbita. Lo stabilizzanze di una collana in S_{10} è dato dalle $3! \cdot 3! \cdot 4!$ permutazioni che permutano tra loro (senza mescolare colori diversi) le 3 perline rosse, le 3 blu e le 4 gialle. In totale possiamo disegnare $\frac{10!}{3! \cdot 3! \cdot 4!} = 4200$ collane diverse tra loro su di un foglio di carta. Tra queste però molte sono sovrapponibili con un'isometria che manda il decagono in sé stesso. Diremo che due collane siffatte sono equivalenti. Siamo pertanto interessati a trovare il numero delle classi di equivalenza, ovvero le orbite del gruppo D_{20} delle isometrie del decagono sull'insieme delle collanine disegnabili. Per fare questo ci viene in aiuto la formula di Burnside. Ricordiamo che D_{20} è composto dall'identità, che fissa tutte le 4200 collanine, da nove rotazioni di un multiplo dell'angolo $\pi/5$ e da dieci riflessioni rispetto agli assi di simmetria del decagono regolare. Notiamo che nessuna rotazione non identica fissa una qualche collanina. Una riflessione che mandi una collanina in sé deve avere necessariamente l'asse

passante per un vertice blu ed ed uno rosso (dovendo scambiare vertici dello stesso colore) ed è pertanto una delle 5 riflessioni rispetto alle congiungenti i vertici opposti del decagono. Vi sono in questo caso (fissata la riflessione) $2\binom{4}{2}\binom{2}{1}$ modi di assegnare i colori dei due vertici fissati, delle posizioni delle 2 coppie di palline gialle tra quattro posizioni possibili ed una tra le due posizioni rimanenti per la coppia di palline rosse (la coppia di palline blu ha a questo punto una posizione assegnata). Le riflessioni attorno all'asse di un lato del decagono non fissano alcuna collana. Il numero t delle orbite si calcola allora con la formula di Burnside:

$$t = \frac{1}{20}\left(4200 + 5 \cdot 2 \cdot \binom{4}{2}\binom{2}{1}\right) = 216$$

È possibile controllare la validità di questo esempio utilizzando il programma GAP (disponibile nei laboratori del centro di calcolo) come mostrato nella Tabella 3.1.

3.4 Omomorfismi e sottogruppi normali.

Abbiamo già incontrato la nozione di isomorfismo. Un concetto più debole è quello di omomorfismo.

Definizione 3.17. Dati due gruppi G e G', Una funzione definita su di un gruppo $f\colon G \to G'$ è detta omomorfismo se $f(gh) = f(g)f(h)$.

Proposizione 3.18. *Si consideri un omomorfismo $f\colon G \to G'$. Allora*

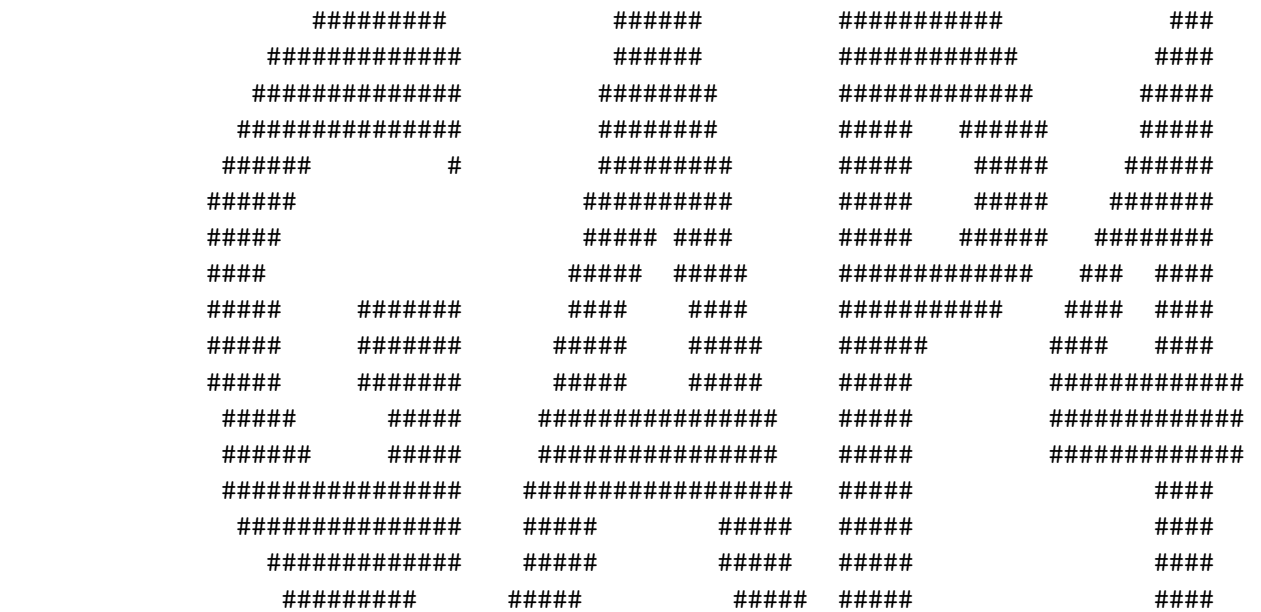
1. $f(1) = 1$;
2. *per ogni $g \in G$ e per ogni $m \in \mathbb{Z}$ si ha $f(g^m) = f(g)^m$;*
3. *per ogni sottogruppo $H \leq G$ l'immagine $f(H) = \{\, f(h) \mid h \in H \,\}$ è un sottogruppo di G';*
4. *per ogni sottogruppo $S \leq G'$ la controimmagine*

$$f^{-1}(S) = \{\, g \in G \mid f(g) \in S \,\}$$

è un sottogruppo di G'.

Dimostrazione. 1.

$$f(1) = f(1)(f(1)f(1)^{-1}) = f(1 \cdot 1)f(1)^{-1} = f(1))f(1)^{-1} = 1.$$



```
    Information at:  http://www-gap.dcs.st-and.ac.uk/~gap
    ? for help. Copyright and authors list by ?copyright, ?authors

   Loading the library. Please be patient, this may take a while.
GAP4, Version: 4r2 fix8 of 7-June-2001, i586-pc-linux-gnu-gcc
Components:  small, small2, small3, small4, small5, small6, small7,
             small8, id2, id3, id4, id5, id6, trans, prim, tbl,
             tom  installed.
gap> g:=Group((1,2,3,4,5,6,7,8,9,10),(2,10)*(3,9)*(4,8)*(5,7));
Group([ ( 1, 2, 3, 4, 5, 6, 7, 8, 9,10), ( 2,10)( 3, 9)( 4, 8)( 5, 7) ])
gap> Size (g);
20
gap> x:=Orbit(SymmetricGroup(10), [1,1,1,1,2,2,2,3,3,3], Permuted);;
gap> orbs:=Orbits(g, x, Permuted);;
gap> Size(orbs);
216
gap>
```

Tabella 3.1: Breve sessione con GAP

2. Per $m = 0$ si tratta dell'asserto precedente. Se $m > 0$ allora

$$f(g^m) = f(\underbrace{g \cdots g}_{m \text{ volte}}) = \underbrace{f(g) \cdots f(g)}_{m \text{ volte}} = f(g)^m.$$

Se $m = -1$ allora

$$1 = f(gg^{-1}) = f(g)f(g^{-1}).$$

Dall'unicità dell'inverso di un elemento in un gruppo si trova $f(g^{-1}) = f(g)^{-1}$. Infine se $m < 0$, per quanto appena mostrato, si ha

$$f(g^m) = f((g^{-1})^{-m}) = f(g^{-1})^{-m} = (f(g)^{-1})^{-m} = f(g)^m$$

3. $1 = f(1) \in f(H)$ cosicché $f(H) \neq \emptyset$. Inoltre presi due generici elementi $f(h)$ ed $f(k)$ di $f(H)$, dove $h, k \in H$, si ha $f(h)f(k)^{-1} = f(hk^{-1}) \in f(H)$, dimostrando così che $f(H)$ è un sottogruppo di G'.

4. $1 = f(1) \in S$ e quindi $1 \in f^{-1}(S)$. In particolare $f^{-1}(S)$ non è vuoto. Inoltre presi comunque due elementi g ed h in $f^{-1}(S)$ si ha $f(gh^{-1}) = f(g)f(h)^{-1} \in S$ poiché $f(g)$ e $f(h)$ per ipotesi sono due elementi di S. Pertanto $gh^{-1} \in f^{-1}(S)$.

□

Immediate conseguenza di questa proposizione sono i seguenti fatti: $f(G)$ è un sottogruppo di G' e $K = f^{-1}(\{\,1\,\})$ è un sottogruppo di G. Il sottogruppo K viene anche detto *nucleo di* f e viene denotato con

$$\ker f := \{\, g \in G \mid f(g) = 1 \,\}.$$

Proposizione 3.19. *Un omomorfismo tra due gruppi $f\colon G \to G'$ è iniettivo se e solo* $\ker f = \{\,1\,\}$.

Dimostrazione. f è una funzione iniettiva allora l'elemento neutro di G' ammette come unica controimmagine l'elemento neutro di G e pertanto $\ker f = \{\,1\,\}$. Viceversa supponiamo che $\ker f = \{\,1\,\}$ e che $f(g) = f(h)$. Allora si ha $1 = f(g)f(h)^{-1} = f(gh^{-1})$. Pertanto $gh^{-1} \in \ker f = \{\,1\,\}$ e quindi $gh^{-1} = 1$. Se ne deduce che $g = h$ ed f è una funzione iniettiva. □

Proposizione 3.20. *Sia $f\colon G \to G'$ un omomorfismo tra due due gruppi e sia $K = \ker f$. Allora $f(g) = f(h) = y$ se e solo se $gK = Kh$. In particolare, per $h = g$, si ottiene che per ogni $g \in G$ vale $gK = Kg = \{\, h \in G \mid f(h) = f(g) \,\} = f^{-1}(\{\, y \,\})$.*

Dimostrazione. Cominciamo a supporre che $f(g) = f(h)$ e che $k \in K$. Allora $f(gkh^{-1}) = f(g)f(k)f(h)^{-1} = f(g) \cdot 1 \cdot f(g)^{-1} = 1$. Questo implica che $k' = gkh^{-1} \in K$. Pertanto $gk = k'h \in Kh$ e quindi $gK \subseteq Kh$. In modo analogo, calcolando $f(g^{-1}kh)$, si vede che vale l'inclusione opposta $Kh \subseteq gK$. □

Definizione 3.21. Un sottogruppo N di un gruppo G è detto sottogruppo normale di G se per ogni $g \in G$ si ha $gN = Ng$. Useremo la scirttura $N \trianglelefteq G$ per indicare che N è un sottogruppo normale di G.

In base a questa definizione ed alla Proposizione 3.20 si ottiene immediatamente il seguente corollario.

Corollario 3.22. *Il nucleo di un omomorfismo $f\colon G \to G'$ è un sottogruppo normale di G.*

Un modo semplice per stabilire se un sottogruppo di un gruppo è un sottogruppo normale è fornito dalla seguente proposizione.

Proposizione 3.23. *Un sottogruppo $N \leq G$ è un sottogruppo normale di G se e solo se per ogni $g \in G$ e per ogni $n \in N$ si ha $g^{-1}ng \in N$.*

Dimostrazione. Supponiamo che $N \trianglelefteq G$ e che $n \in N$ e $g \in G$. Poiché $ng \in Ng = gN$ esiste un elemento $n' \in N$ tale che $ng = gn'$. Pertanto $g^{-1}ng = g^{-1}(ng) = g^{-1}(gn') = n' \in N$.

Viceversa se supponiamo che per ogni $g \in G$ e per ogni $n \in N$ si ha $n' = g^{-1}ng \in N$ avremo $ng = g(g^{-}ng)g = gn' \in gN$ che implica $Ng \subseteq gN$. Analogamente $gn = (g^{-1})^{-1}n = (g^{-1})^{-1}ng^{-1}(g^{-1})^{-1} = n''g$, dove $n'' = (g^{-1})^{-1}ng^{-1} \in N$, mostrando così che vale l'inclusione opposta $gN \subseteq Ng$. □

3.4.1 Esempi di sottogruppi normali

- Il sottogruppo $\mathrm{SL}(n,\mathbb{R}) = \{\, M \in \mathrm{GL}(n,\mathbb{R}) \mid \det M = 1 \,\}$ è un sottogruppo normale di $\mathrm{GL}(n,\mathbb{R})$. Infatti la funzione $\det \mathrm{GL}(n,\mathbb{R}) \to \mathbb{R}^*$ che associa ad una matrice invertibile il suo determinante è un omomorfismo: $\det(MN) = \det(M)\det(N)$. Il sottogruppo $\mathrm{SL}(n,\mathbb{R})$ è il nucleo di tale omomorfismo ed è pertanto un sottogruppo normale di $\mathrm{GL}(n,\mathbb{R})$.

- Il sottogruppo A_n delle permutazioni pari di S_n è il nucleo dell'omomorfismo $\mathrm{sgn}\colon S_n \to \mathbb{R}^*$ che associa ad una permutazione il suo segno.

- Sia X un G-insieme, allora il sottoinsieme

$$G_X = \{\, g \in G \mid \text{per ogni } x \text{ in } X \text{ si ha } gx = x \,\}$$

è un sottogruppo normale di G. Infatti G_X non è vuoto contenendo l'elemento neutro di G e se $g, g' \in G$ allora per ogni $x \in X$ si ha $g(g')^{-1}x = x$ e pertanto $g(g')^{-1} \in G_X$, il che mostra che G_X è un

sottogruppo. Esso è anche normale in G infatti per ogni $g \in G$ e per ogni $n \in G_X$ si ha che comunque si scelga $x \in X$ vale $(g^{-1}ng)x = g^{-1}(n(gx)) = g^1(gx) = x$, mostrando in tal modo che $g^{-1}ng \in G_X$ (quindi G_X è normale per la Proposizione 3.23).

- Un sottogruppo $H \leq G$ che ha soli due laterali in G è normale in G. Sia $X = \{ g_1H, g_2H \}$ l'insieme dei laterali destri (il caso dei laterali sisnistri è lasciato al lettore) di H in G. Se $x = tH \in X$ definiamo $g \cdot x = (gt)H$. In tal modo G agisce su X e X diviene un G-insieme. Notiamo che si può scegliere $g_1 = 1$. Quindi $g \in G$ fissa g_1H (e quindi necessariamente anche g_2H) se e solo se $g \in H$. Pertanto $H = G_X$ è un sottogruppo normale di G per quanto visto nell'esempio precedente.

Esercizio 3.5. Dimostrare che se $H \leq G$ e $N \trianglelefteq G$ allora $H \cap N \trianglelefteq H$.

Esercizio 3.6. Dimostrare in un gruppo abeliano tutti i sottogruppi sono normali.

Esercizio 3.7. Posto $G = S_4$, $V = \{ \mathrm{Id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) \}$ e $H = \{ \mathrm{Id}, (1,2)(3,4) \}$, dimostrare che H è un sottogruppo normale di V, che V è un sottogruppo normale di G ma che H non è un sottogruppo normale di G.

Esercizio 3.8. Dato un sottogruppo H di G ed un elemento $g \in G$ si definisce $g^{-1}Hg = \{ g^{-1}hg \mid h \in H \}$. Dimostrare che

1. $g^{-1}Hg$ è un sottogruppo di G.
2. un sottogruppo $N \leq G$ è un sottogruppo normale di G se e solo se per ogni $g \in G$ si ha $g^{-1}Ng = N$

3.5 Gruppi quozienti

Torniamo alla costruzione delle classi di resto modulo n. La classe di resto $[x]_n$ di un intero x è data da tutti gli interi che si ottengono da x aggiungendo un multiplo di n: $[x]_n = \{ x + kn \mid k \in \mathbb{Z} \} = x + n\mathbb{Z}$. Ovvero una classe di resto modulo n non è altro che un laterale del sottogruppo $n\mathbb{Z}$ di $\mathbb{Z}$.

Mettiamoci ora nella situazione più generale in cui si ha un gruppo G ed un suo sottogruppo normale N (vedremo poi perché è importante che sia normale), imitando la costruzione delle classi di resto modulo n definiamo l'insieme G/N, che per ora chiamiamo insieme delle classi di resto degli elementi di G modulo N, ponendo G/N uguale all'insieme dei laterali di N in G (non importa destri o sinistri visto il fatto che N è normale). Allo stesso

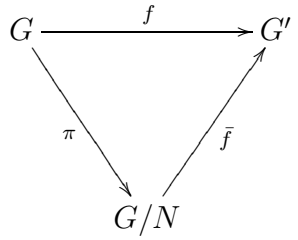
modo in cui si definisce l'operazione di somma di classi di resto modulo n definiamo l'operazione di *prodotto di laterali* in G/N ponendo $gN \cdot hN = ghN$. Notiamo che se si ha $gN = g'N$ e $hN = h'N$ allora $g' = gm$ e $h' = hn$ per qualche $n, m \in N$. Pertanto $g'h' = gmhn = gh\underbrace{(h^{-1}mh)n}_{\in N}$ (qui si usa il fatto che $N \trianglelefteq G$ per poter affermare che $h^{-1}mh \in N$) e quindi $g'h'N = ghN$ di modo che l'operazione di prodotto di laterali è ben definita in G/N.

È facile vedere che l'operazione definita in G/N è associativa, ammette il laterale $1N = N$ come elemento neutro, inoltre ogni laterale gN ammette $g^{-1}N$ come inverso rispetto a questa operazione. Pertanto G/N munito dell'operazione di prodotto di laterali risulta essere un gruppo detto *gruppo quoziente di G modulo N*.

Torniamo all'esempio di partenza se $n > 1$ è un intero il gruppo delle classi di resto modulo n rispetto alla somma di classi di resto coincide con il gruppo quoziente $\mathbb{Z}/n\mathbb{Z}$.

Esiste sempre un omomorfismo, detto proiezione canonica sul quoziente, $\pi\colon G \to G/N$ definito da $\pi(g) = gN$. Il nucleo di tale omomorfismo è $\ker \pi = \{\, g \in G \mid gN = N \,\} = N$. Pertanto ogni sottogruppo normale è il nucleo di qualche omomorfismo.

Teorema 3.24 (Teorema Fondamentale dell'Isomorfismo)**.** *Dati due gruppi G e G' ed un omomorfismo $f\colon G \to G'$ avente nucleo $\ker f = N$, esiste un unico isomorfismo $\bar{f}\colon G/N \to f(G)$ tale che $f = \bar{f} \circ \pi$. In particolare l'immagine di f è un gruppo isomorfo a G/N.*



Dimostrazione. La funzione $\bar{f}$ è univocamente determinata in quanto deve essere $\bar{f}(gN) = \bar{f}(\pi(g)) = f(g)$. Ne segue che l'immagine di $\bar{f}$ coincide con l'immagine di f. Si ha anche che $\bar{f}(gN \cdot hN) = \bar{f}(ghN) = f(gh) = f(g)f(h) = \bar{f}(gN)\bar{f}(hN)$ e pertanto $\bar{f}$ è un omomorfismo. Resta solo da mostrare che $\bar{f}$ è iniettiva. Calcoliamone il nucleo: $\ker \bar{f} = \{\, gN \in G/N \mid f(g) = 1 \,\} = \{\, N \,\} = \{\, 1_{G/N} \,\}$. Questo mostra che $\bar{f}$ è un omomorfismo iniettivo. □

Corollario 3.25. *Un gruppo ciclico $G = \langle\, x \,\rangle$ è isomorfo al gruppo delle classi di resto $\mathbb{Z}/n\mathbb{Z}$ se è finito di ordine n, altrimenti è isomorfo a $\mathbb{Z}$.*

Dimostrazione. L'applicazione $f\colon \mathbb{Z} \to G$ definita da $f(m) = x^m$ è suriettiva essendo $G = \langle\, x \,\rangle = \{\, x^m \mid m \in \mathbb{Z} \,\} = f(\mathbb{Z})$. Tale applicazione è un omomorfismo di gruppi, infatti per ogni n ed m in $\mathbb{Z}$ vale $f(m+n) = x^{n+m} = x^n y^m = f(n)f(m)$. Se G è finito f non può essere iniettiva (perché il dominio di f è un insieme infinito) e pertanto dal Teorema 3.6 si ha $0 \neq \ker f = n\mathbb{Z}$ con $n > 0$. Dal Teorema Fondamentale dell'Isomorfismo abbiamo che $G = f(\mathbb{Z})$ è isomorfo a $\mathbb{Z}/n\mathbb{Z}$ ed ha pertanto lo stesso numero n di elementi di $\mathbb{Z}/n\mathbb{Z}$.

D'altra parte f è iniettivo solo se G è infinito ed in tal caso f è un isomorfismo di $\mathbb{Z}$ in G. □

Capitolo 4

Anelli

4.1 Gli anelli

Prerequisiti: la parte del corso di elementi matematica riguardanti i polinomi, il teorema di Ruffini, la divisione tra polinomi e la fattorizzazione di polinomi.

4.1.1 Definizioni ed esempi

Alcune strutture algebriche che conosciamo hanno più di un'operazione si pensi ad esempio ai numeri interi, ai numeri reali o alle classi di resto modulo n. Diamo pertanto una definizione che ne accomuni le proprietà.

Definizione 4.1. Un insieme $(A, +, \cdot)$ dotato di due operazioni, dette somma e prodotto, è detto anello se

1. A è un gruppo abeliano rispetto all'operazione di somma (che si scrive in notazione additiva), il cui elemento neutro è detto zero dell'anello ed è denotato con 0 o con 0_A,
2. l'operazione di prodotto (in notazione moltiplicativa) è associativa ed ammette un elemento neutro, detto uno e denotato con 1 o con 1_A,
3. vale la legge distributiva del prodotto rispetto alla somma: per ogni terna di elemento $a, b, c \in A$ si ha $a(b+c) = ab+ac$ e $(b+c)a = ba+ca$,
4. $1 \neq 0$.

Sel'operazione di prodotto definita in A gode della proprità commutativa diremo che A è un anello commutativo.

Sono esempi di anelli i seguenti:

Gli interi. L'insieme $\mathbb{Z}$ dei numeri interi rispetto alla somma ed al prodotto usuali di numeri interi.

I numeri razionali. L'insieme $\mathbb{Q}$ dei numeri razionali rispetto alla somma ed al prodotto usuali di numeri razionali.

I numeri reali. L'insieme $\mathbb{R}$ dei numeri reali rispetto alla somma ed al prodotto usuali di numeri reali.

I numeri complessi. L'insieme $\mathbb{C}$ dei numeri complessi rispetto alla somma ed al prodotto usuali di numeri complessi.

Le classi di resto modulo n. L'insieme $\mathbb{Z}_n$ delle classi di resto dei numeri interi modulo n rispetto alla somma ed al prodotto usuali di classi di resto.

Le matrici reali n per n. L'insieme $M_n(\mathbb{R})$ delle matrici a coefficienti reali di resto rispetto alla somma ed al prodotto usuali di matrici (anello non commutativo).

Esercizio 4.1. Dimostrare che se A è un anello allora per ogni coppia di elementi $a, b \in A$ e per ogni intero $m \in \mathbb{Z}$ valgono le identità:

1. $a \cdot 0 = 0 \cdot a = 0$,
2. $a \cdot (-b) = (-b)cdota = -ab$,
3. $(ma) \cdot b = a \cdot (mb) = m(ab)$.

Definizione 4.2. Un anello commutativo A è detto essere un dominio se l'insieme $A^* = \{ a \in A \mid a \neq 0 \}$ è chiuso rispetto al prodotto, overo se il prodotto di due elementi di A diversi da zero è un elemento di A diverso da 0.

Definizione 4.3. Un anello commutativo A è detto essere un campo se l'insieme $A^* = \{ a \in A \mid a \neq 0 \}$ è chiuso rispetto al prodotto e rispetto a tale operazione risulta essere un gruppo.

Lasciamo al lettore il compito di mostrare che per mostrare che un anello A è un campo è sufficiente mostrare che per ogni $a \in A^*$ esiste un elemento (che risulta essere necessariamente unico) $b \in A$ tale che $ab = 1$. Dalla definizione di campo si ottiene subito che ogni campo è anche un dominio.

Tra gli esempi elencati risultano essere campi $\mathbb{R}$, $\mathbb{C}$ e $\mathbb{Q}$. L'anello $\mathbb{Z}$ è un dominio. Per quel che riguarda le classi di resto modulo n abbiamo il seguente risultato.

Proposizione 4.4. *Sia $n \geq 2$ un intero. Allora le seguenti affermazioni sono equivalenti:*

1. *$\mathbb{Z}_n$ è un campo,*
2. *$\mathbb{Z}_n$ è un dominio,*
3. *n è un numero primo.*

Dimostrazione. Chiaramente (1) implica (2).

Mostriamo che (2) implica (3). Supponiamo per assurdo che si possa scrivere $n = pq$ dove $1 < p \leq q < n$. Alora le classi di resto $[p]_n$ e $[q]_n$ sono entrambe diverse dalla classe nulla $[0]_n$. Poiché stiamo supponendo che $\mathbb{Z}_n$ sia un dominio troviamo una contraddizione: $[0]_n \neq [p]_n \cdot [q]_n = [pq]_n = [n]_n = [0]_n$. Pertanto non può esistere una fattorizzazione non banale di n che risulta in tal modo essere un numero primo.

Sappiamo già, dal Teorema 1.19, che (3) implica (1). □

4.1.2 Ideali ed omomorfismi di anelli

Così come si è fatto per i gruppi è possibile introdurre il concetto di omomorfismo di anelli.

Definizione 4.5. Un omomorfismo f da un anello A in un anello B è una funzione $f\colon A \to B$ tale che,

1. Per ogni $x, y \in A$ si ha $f(x + y) = f(x) + f(y)$ (f è un omomorfismo del gruppo additivo $(A, +)$ nel gruppo additivo $(B, +)$),
2. Per ogni $x, y \in A$ si ha $f(xy) = f(x)f(y)$,
3. $f(1_A) = 1_B$.

Il nucleo di f viene denotato con $\ker f$ e coincide con il nucleo dell'omomorfismo f tra i gruppi additivi dei due anelli: $\ker f = \{\, x \in A \mid f(x) = 0 \,\}$. Un omorfismo biunivoco è detto isomorfismo. Due anelli A e B sono detti tra loro iso se esiste un isomorfismo $f\colon A \to B$. Si lascia al lettore di verificate che la funzione inversa di un omomorfismo è un omomorfismo.

Esempi di omomorfismi sono i seguenti.

- La funzione $f\colon \mathbb{Z} \to \mathbb{Z}_n$ definita da $f(m) = [m]_n$ è un omomorfismo di anelli.

- Se A è un anello, allora la funzione $f\colon \mathbb{Z} \to A$ definita da $f(m) = m \cdot 1_A$ è un omomorfismo di anelli. L'immagine di questa funzione è un sottoanello di A (sottoinsieme che risulta essere un anello rispetto alle stesse operazioni definite in A e contenente 1_A) detto sottoanello fondamentale di A denotato anche con $\mathbb{Z}1_A = \{\, m \cdot 1_A \mid m \in \mathbb{Z} \,\}$.

Definizione 4.6. Un ideale (bilatero) I di un anello A è un sottoinsieme di A tale che:

1. risulti essere un sottogruppo rispetto all'operazione di somma,
2. goda della proprietà di assorbimento: per ogni $a \in A$ e per ogni $x \in I$ si deve avere $ax \in I$ e $xa \in I$.

Gli ideali di un anello hanno lo stesso ruolo dei sottogruppi normali nei gruppi come sarà evidente da quanto segue.

Proposizione 4.7. *Il nucleo I di un omomorfismo di anelli $f\colon A \to B$ è un ideale di A.*

Dimostrazione. I è un sottogruppo di $(A, +)$ in quanto è il nucleo di f visto come omomorfismo tra i due gruppi additivi $(A, +)$ e $(B, +)$. Per ogni $a \in A$ ed ogni $i \in I$ si ha $f(ai) = f(a)f(i) = f(a)\cdot 0 = 0$ ed analogamente $f(ia) = 0$. Pertanto gli elementi ai ed ia appartengono al nucleo I di f. □

Come nel caso dei gruppi si può dare una struttura di anello all'insieme $A/I = \{\, I + a \mid a \in A \,\}$ dei laterali di un ideale I (visto come sottogruppo di $(A, +)$). Definiremo la somma di due laterali $I + a$ e $I + b$ ponendo $(I + a) + (I + b) = I + (a + b)$. Analogamente definiamo il loro prodotto $(I+a)(I+b) = I+ab$. Tali operazioni sono ben definite. Infatti supponiamo che $a+I = a'+I$ e che $b+I = b'+I$. Allora $a-a' \in I$ e $b-b' \in I$ per cui $(a+b)-(a'+b') = (a-a')+(b-b') \in I$. Ne consegue che $I+(a+b) = I+(a'+b')$. Analogamente $ab-a'b' = \underbrace{(a-a')}_{\in I}(b+b') - \underbrace{(a-a')}_{\in I}b' + a'\underbrace{(b-b')}_{\in I} \in I$ cosicché $I + ab = I + a'b'$. Viene lasciato al lettore di verificare che l'insieme A/I, fornito delle operazioni descritte, risulta esere un anello in cui $0_{A/I} = I = I+0$ e $1_{A/I} = I + 1$.

Come nel caso dei gruppi la proiezione canonica sul quoziente $\pi\colon A \to A/I$ definita da $\pi(a) = a + I$ risulta essere un omomorfismo suriettivo di anelli il cui nucleo è I. Vale anche il teorema fondamentale dell'isomorfismo per gli anelli (la cui dimostrazion è analoga a quella descritta nel caso dei gruppi).

Teorema 4.8. *Dati due anelli A e B ed un omomorfismo $f\colon A \to B$ avente per nucleo un ideale I esiste un unico isomorfismo iniettivo $\bar{f}\colon A/I \to f(A)$ tale che $f = \bar{f} \circ \pi$. Tale isomorfismo è definito da $\bar{f}(I + a) = f(a)$. In paticolare $f(A)$ è un sottoanello di B isomorfo ad A/I.*

4.1.3 Ideali di $\mathbb{Z}$

Ci proponiamo ora di determinare tutti gli dieali di $\mathbb{Z}$. Un ideale di $\mathbb{Z}$ è anche un suo sottogruppo additivo e pertanto, in base al Teorema 3.6 esiste un intero $n \geq 0$ tale che $I = n\mathbb{Z} = \{ nx \mid x \in \mathbb{Z} \}$. Viceversa, comunque scelto $n \in Z$, il sottoinsieme $I = n\mathbb{Z} = \{ nx \mid x \in \mathbb{Z} \}$ risulta essere un ideale in $\mathbb{Z}$. Infatti esso è un sottogruppo di $\mathbb{Z}$ e per ogni $m \in \mathbb{Z}$ e per ogni $i = nx \in I$ si ha $im = mi = mnx = n(mx) \in n\mathbb{Z} = I$.

Pertanto gli ideali di $\mathbb{Z}$ sono tutti e soli i sottoinsiemi della forma $n\mathbb{Z}$ dove n è un intero.

4.2 Anelli di polinomi

In questo paragrafo supporremo che R sia un anello commutativo. Un polinomio $p(x)$ a coefficienti in R nell'indeterminata (o variabile) x è una scrittura del tipo $p(x) = a_0 + a_1 x + \cdots a_n x^n$ dove $a_i \in R$ per $i = 1, \ldots, n$. Per comodità scriveremo anche $p(x) = \sum_{i=0}^{\infty} a_i x^i$ dove supporremo che esiste un intero non negativo n tale che $a_i = 0$ per $i > n$ (solo un numero finito di coefficienti è diverso da 0). L'insieme dei polinomi a coefficienti in R viene denotato con $R[x]$. Possiamo definire la somma ed il prodotto di due polinomi $p(x) = \sum_{i=0}^{\infty} a_i x^i$ e $q(x) = \sum_{i=0}^{\infty} b_i x^i$ ponendo $p(x) + q(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$ e $p(x)q(x) = \sum_{i=0}^{\infty} c_i x^i$ dove $c_i = \sum_{h=0}^{i} a_h b_{i-h}$. Il polinomio nullo (che ha tutti i coefficienti uguali allo zero di R) è l'elemento neutro rispetto della somma somma il polinomio $1 = 1 + 0 \cdot x + 0 \cdots^2 + \cdots$ è l'elemento neutro del prodotto. Con le operazioni di somma e prodotto di polinomi $R[x]$ acquista una struttura di anello commutativo.

Il grado di un polinomio $p(x) = \sum_{i=0}^{\infty} a_i x^i \neq 0$ è denotato con $\deg p(x)$ e definto come $\deg p(x) = \max \{ i \mid a_i \neq 0 \}$; se il poninomio $p(x)$ ha grado n allora il suo coefficiente a_n di grado massimo è detto coefficiente direttore di $p(x)$. Un polinomio non nullo è detto monico se il suo coefficiente direttore è uguale a 1.

Proposizione 4.9. *Siano $g(x)$ ed $h(x)$ due polinomi a coefficienti nell'anello R, allora se $g(x)h(x) \neq 0$ si ha $\deg(g(x)h(x)) \leq \deg g(x) + \deg h(x)$. Nel caso in cui R sia un dominio vale $\deg(g(x)h(x)) = \deg g(x) + \deg h(x)$, in particolare $R[x]$ è a sua volta un dominio.*

Dimostrazione. Supponiamo che $g(x) = \sum_{i=0}^{\infty} a_i x^i$ e $h(x) = \sum_{i=0}^{\infty} b_i x^i$ abbiano gradon m ed n rispettivamente, e quindi che $a_i = 0$ per $i > m$ e $b_j = 0$ per $j > n$. Poniamo $s(x) = \sum_{i=0}^{\infty} c_i x^i = g(x)h(x)$ e supponiamo che $s(x) \neq 0$. Supponiamo che $i > m + n$, allora dalla formula per il prodotto di

due polinomi abbiamo

$$c_i = \sum_{j=0}^{i} a_j b_{i-j} \tag{4.1}$$

Poiché si ha che o $j > m$ o $i - j > n + m - j \geq n + m$ trova che per $j \leq m$ si ha $b_{i-j} = 0$, mentre per $j > m$ si ha $a_j = 0$. In particolare ogni addendo della sommatoria in (4.1) è uguale a 0 e pertanto $c_i = 0$ per $i > n + m$ il che è equivalente ad asserire che $\deg s(x) \leq n + m$.

Se R è un dominio allora, tenendo conto che $a_i = 0$ per $i > m$ e che $b_j = 0$ per $j > n$, si trova $c_{n+m} = a_m b_n \neq 0$ dimostrando in tal modo che $\deg s(x) >\geq n + m$. Siccome abbiamo dimostrato che vale la diseguaglianza opposta vale l'uguaglianza $\deg s(x) = \deg g(x) + \deg h(x)$. □

Esercizio 4.2. Dimostrare che $R[x]$ è un dominio se e solo se R è un dominio.

Dato un polinomio $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ ed un elemento $\alpha \in K$ chiameremo *valutazione di* $p(x)$ *in* α l'elemento di R denotato con $p(\alpha)$ o con $p(x)|_{x=\alpha}$ definito da $p(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$. Si lascia al lettore di verificare che se $a(x)$ e $b(x)$ sono due elementi di $R[x]$, posto $p(x) = a(x)b(x)$ e $s(x) = p(x) + q(x)$, valgono le uguaglianze:

$$p(\alpha) = a(\alpha)b(\alpha) \tag{4.2}$$
$$s(\alpha) = a(\alpha) + b(\alpha) \tag{4.3}$$

4.2.1 Anelli di polinomi a coefficienti in un campo

In questo paragrafo K denoterà un campo. L'algoritmo della divisione tra polinomi a coefficienti reali presentato nel corso di elementi di matematica di può applicare a due polinomi purché siano a coefficienti in un campo K, in tal modo il quoziente ed il resto della loro divisione sono anch'essi polinomi nello stesso campo K. Valgono infatti i seguenti risultati che si dimostrano in modo identico al caso dei polinomi reali.

Teorema 4.10. *Dati due polinomi $a(x)$ e $b(x)$ nell'anello $K[x]$, dove $b(x) \neq 0$, esistono due polinomi $q(x)$ ed $r(x)$, detti quoziente e resto della divisione di $a(x)$ per $b(x)$, tali*

1. $a(x) = b(x)q(x) + r(x)$,
2. *se* $r(x) \neq 0$ *allora* $\deg r(x) < \deg b(x)$.

Se il resto della divisione di $a(x)$ per $b(x)$ è nullo e quindi $a(x) = b(x)q(x)$ diremo che $b(x)$ divide (o è un divisore di) $a(x)$.

Definizione 4.11. Un elemento $\alpha \in K$ è detto radice di un polinomio $p(x) \in K[x]$ se $p(\alpha) = 0$.

Teorema 4.12 (di Ruffini)**.** *Dati un polinomio $p(x) \in K[x]$ e un elemento $\alpha \in K$ allora $p(\alpha) = r$ dove r è il resto della divisione di $p(x)$ per $x - \alpha$. In particolare $p(x)$ è divisibile per $x - \alpha$ se e solo se α è una radice di $p(x)$.*

Definizione 4.13. Un polinomio $p(x) \in K[x]$ di grado maggiore di 0 è detto irriducible se ogniqulavolta esistano due polinomi $a(x)$ e $b(x)$ in $K[x]$ tali che $\deg a(x) > 0$ e che $p(x) = a(x)b(x)$ allora si ha $\deg a(x) = \deg p(x)$ e $\deg b(x) = 0$. Ovvero i soli divisori di $p(x)$ sono i polinomi costanti e quelli della forma $\alpha p(x)$ con $\alpha \in K$.

La dimostrazione del seguente teorema è analoga alla dimostrazione dellla fattorizzazione degli interi in fattori primi e pertanto viene omessa.

Teorema 4.14 (della fattorizzazione unica)**.** *Per ogni polinomio $a(x) \in K[x]$ esistono e sono univocamente determinati un numero finito di polinomi irriducibili monici ed a due a due distinti $p_1(x), \ldots, p_k(x) \in K[x]$, una k-upla di interi positivi $(e_1, \ldots, e_k) \in \mathbb{Z}^k$ e un elemento $\alpha \in K$ tali che $a(x) = \alpha p_1(x)^{e_1} \cdots p_k(x)^{e_k}$.*

Corollario 4.15 (Teorema di Wilson)**.** *Sia p un numero primo, allora $(p-1)! \equiv -1 \bmod p$.*

Dimostrazione. Poiché per il teorema di Eulero si ha che ogni elemento in $\mathbb{Z}_p^*$ è radice del polinomio $x^{p-1} - 1 \in \mathbb{Z}_p[x]$, dal Teorema di Ruffini e dal teorema precedente si ricava $x^{p-1} - 1 = (x-1)(x-2)\cdots(x-p+1)$ (in $\mathbb{Z}_p[x]$). Valutando entrami i membri per $x = 0 \equiv p \bmod p$ si trova $-1 \equiv (p-1)(p-2)\cdots 2 \cdot 1 = (p-1)! \bmod p$. □

Un massimo comun $d(x)$ divisore di due polinomi $a(x)$ e $b(x)$ in $K[x]$ è definito in modo analogo al massimo comun divisore di due interi. Esso pertanto è definito dal fatto di godere delle seguenti proprietà:

1. $d(x)$ divide $a(x)$ e $b(x)$,
2. se $c(x) \in K[x]$ è un divisore comune di $a(x)$ e $b(x)$ allora $c(x)$ è anche un divisore di $d(x)$.

Dalla seconda proprietà discende che due massimi comun divisori di due polinomi si devono dividere a vicenda e pertanto si possono ottenere l'uno dall'altro tramite la moltiplicazione per una costante α non nulla (esercizio). In ogni caso vi è un unico massimo comun divisore di due polinomi $a(x)$

e $b(x)$ non entrambi nulli, che risulti essere monico. L'algoritmo di Euclide delle divisioni successive, che si basa sulla divisione con resto, permette di calcolare il massimo comu divisore anche nel caso dei polinomi. Vale il seguente risultato analogo a quello che si ottiene per i numeri interi.

Teorema 4.16 (di Bezout)**.** *Dati due polinomi $a(x)$ e $b(x)$ in $K[x]$ esiste almeno un loro massimo comun divisore $d(x)$. I massimi comuni divisori di $a(x)$ e $b(x)$sono tutti i polinomi della forma $\alpha d(x)$ al variare di $\alpha \in K^* = K \setminus \{0\}$. Esistono inoltre due polinomi $h(x)$ e $k(x)$ in $K[x]$ tali che $d(x) = a(x)h(x) + b(x)k(x)$.*

Esempio. Troviamo ad esempio con l'algoritmo delle divisioni successive, in $\mathbb{Z}_7[x]$ (si noti che $\mathbb{Z}_7$ è un campo) il massimo comun divisore tra $a(x) = x^4 + 6$ e $b(x) = x^4 + 4x^2 + 2$ e scriviamolo come loro combinazione lineare. Comiciamo a dividere $a(x)$ per $b(x)$:

x^4		$+6$	$x^4 + 4x^2 + 2$
x^4	$+4x^2$	$+2$	1
	$3x^2$	$+4$	

Da cui

$$a(x) = b(x) + r_1(x)$$

dove $r_1(x) = 3x^2 + 4$. Adesso dividiamo $b(x)$ per $r_1(x)$:

x^4	$+4x^2$	$+2$	$3x^2 + 4$
x^4	$+6x^2$		$5x^2 + 4$
	$5x^2$	$+2$	
	$5x^2$	$+2$	
		0	

Troviamo allora che $d(x) = r_1(x) = 3(x^2 - 1)$ è il massimo comun divisore di $a(x)$ e $b(x)$. Inoltre $d(x) = 1 \cdot a(x) + 6 \cdot b(x)$.

4.3 Domini ad ideali principali

Sia R un anello commutativo ed a un suo elemento definiamo $(a) = aR = \{\, ar \mid r \in R \,\}$. Mostriamo che (a) è un ideale di R. Infatti $0 = 0 \cdot a \in (a)$ e pertanto ($a =$ non è vuoto. Inolte scelti due arbitrari elementi ax e ay di (a) (dove $x, y \in R$), si ha $ax - ay = a(x - y) \in (a)$, quindi (a) è un sottogruppo additivo di R. Inoltre, comunque scelti $r \in R$ e $i = ax \in (a)$, si ha $r \cdot i = a(rx) \in (a)$; vale quindi la proprietà di assorbimento ed (a) risuta essere un ideale detto *ideale principale generato da a*. Notiamo che il sottoinsieme $\{\, 0 \,\}$ è l'ideale principale generato da 0.

Definizione 4.17. Un dominio R è detto dominio ad ideali principali se ogni suo ideale I è principale: ovvero esiste $a \in R$ tale che $I = (a)$.

Il paragrafo 4.1.3 mostra che $\mathbb{Z}$ è un dominio ad ideali principali.

Cerchiamo ora di determinare gli ideali di un campo K. Supponiamo che I sia un ideale di K che contenga un qualche elemento $x \neq 0$. Allora, Poiché I è un ideale $1 = x^{-1} \underbrace{(x)}_{\in I} \in I$. Ne consegue che moltilplicando un generico elemento y di K per $1 \in I$ troviamo che $y = y \cdot 1 \in I$. Pertanto $I = K$. Quindi gli ideali di un campo sono solo due $\{\, 0 \,\}$ e K.

Viceversa se A è un anello commutativo con i soli due ideali $\{\, 0 \,\}$ e A allora A è un campo. Infatti se $a \in A$ è un elemento non nullo, allora l'ideale principale generato da a contenendo l'elemento a non può essere $\{\, 0 \,\}$. Di conseguenza $(a) = A$. In particolare $1 \in (a)$ di modoche $1 = ax$ per qualche $x \in A$, mostrando quindi che a ammette x come inverso.Abbiamo allora mostrato la seguente proposizione.

Proposizione 4.18. *Un anello commutativo A è un campo se e solo se A ha i soli due ideali $\{\, 0 \,\} = (0)$ e $A = (1)$. In particolare un campo è un dominio ad ideali principali.*

Teorema 4.19. *Siano K un campo, $I \neq \{\, 0 \,\}$ un ideale dell'anello $K[x]$. Allora esiste un unico polinomio monico $m(x)$ tale che $I = (m(x))$. In particolare $K[x]$ è un dominio ad ideali principali.*

Dimostrazione. Poiché $I \neq 0$ esiste in I un polinomio $p(x) = a_0 + a_1 x + \cdots + a_n x^n \neq 0$ di grado minimo n tra tutti i polinomi di I. Il polinomio $m(x) = \frac{1}{a_n} p(x)$ ha anch'esso grado n, è monico ed appartiene a I. Scelto un polinomio $a(x) \in I$ diviamo $a(x)$ per $m(x)$ ottenendo $a(x) = m(x)q(x) + r(x)$ dove $r(x) = 0$ o $\deg r(x) < n$. Poiché $r(x) = a(x) - m(x)q(x)$ si scrive come differenza di elementi di I anch'esso appartiene a I. Se fosse $r(x) \neq 0$ avrei

in tal modo trovato in I un polinomio non nullo di grado minore di n, contro la scelta fatta di $p(x)$ di essere di grado minimo tra i polinomi non nulli di I. Pertanto $r(x) = 0$ e $a(x) = m(x)q(x)$ appartiene all'ideale generato da $m(x)$. Abiiamo mostrato allora che $I \subseteq (m(x))$. Viceversa se $b(x) = h(x)m(x)$ è un elemento di $m(x)$ abbiamo che che $b(x)$ essendo multiplo di $m(x) \in I$ è anch'esso un elemento di I pertanto $(m(x)) \subseteq I$, da cui $I = (m(x))$.

Supponiamo infine che $\bar{m}(x)$ sia un'altro polinomio monico tale che $I = (m(x)) = (\bar{m}(x))$. Allora $m(x)$, apprtenendo ad $I = (\bar{m}(x))$ è un multiplo di $\bar{m}(x)$ e viceversa $\bar{m}(x)$ è un multiplo di $m(x)$. Ne consegue che $m(x)$ ha lo stesso grado di $\bar{m}(x)$ e pertanto $m(x) = \alpha\bar{m}(x)$ dove $\alpha \in K$. D'altra parte $\alpha = 1$ perché $m(x)$ ed $\bar{m}(x)$ sono entrambi monici. Si ha dunque $m(x) = \bar{m}(x)$ □

Proposizione 4.20. *Sia K un campo ed $I = (m(x))$ un ideale di dell'anello $K[x]$ dove $\deg m(x) = n \geq 1$. Allora ogni laterale di I contiene un unico un polinomio $r(x)$ che risulta essere nullo o di grado minore di n. Ne consegue che tutti e soli i laterali di I sono della forma $I + r(x)$ per un unico $r(x) \in K[x]$ tale che $r(x) = 0$ o $\deg r(x) < n$.*

Dimostrazione. Sia $I + a(x)$ un laterale di

$$I = (m(x)) = \{\, m(x)h(x) \mid h(x) \in K[x] \,\}.$$

Dividiamo $a(x)$ per $m(x)$ e chiamiamo $r(x)$ il resto di tale divisione: $a(x) = q(x)m(x)+r(x)$. Avremo che $a(x)-r(x) = q(x)m(x) \in I$ pertanto $I+a(x) = I + r(x)$ con $r(x) = 0$ o $\deg r(x) < n$.

Se $I + r(x) = I + \bar{r}(x)$ dove $\bar{r}(x)$ è nullo o ha grado minore di n allora $r(x) - \bar{r}(x) \in I = (m(x))$ sarebbe un multiplo di $m(x)$ che, se non è nullo, avrebbe di grado minore del grado di $m(x)$ e questo non è possibile. Pertanto $r(x) - \bar{r}(x) = 0$. □

Corollario 4.21. *Sia p un numero primo e $m(x)$ un polinomio in $\mathbb{Z}_p[x]$ di grado $n \geq 1$, allora la cardinalità di $\mathbb{Z}_p[x]/(m(x))$ è p^n.*

Dimostrazione. Basta notare che per la Proposizione 4.20, i laterali di $(m(x))$ in Z_p sono tanti quanti i polinomi della forma $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. L'asserto segue dal fatto che per ciscuno degli n coefficienti a_i può assumere p valori distinti. □

4.3.1 Classi di resto in $K[x]$

In tutto questo paragrafo K denoterà un campo ed $I = (m(x))$ l'ideale di $K[x]$ generato da un polinomio $m(x)$ di grado maggiore od eguale a 1. L'anello $K[x]/I$ viene detto *anello delle classi di resto modulo $m(x)$*. Infatti un

su elemento che denotiamo con $I + a(x) = \{\, a(x) + m(x)h(x) \mid h(x) in K[x] \,\}$ è una classe di equivalenza i cui elementi sono i polinomi che differiscono da $a(x)$ per un multiplo di $m(x)$. Il prodotto e la somma di due classi di resto $I+a(x)$ e $I+b(x)$ si ottengono considerando le classi del prodotto $I+a(x)b(x)$ e della somma $I + (a(x) + b(x))$ dei rappresentanti $a(x)$ e $b(x)$.

Facciamo subito un esempio. Consideriamo il campo $K = \mathbb{Z}_3$ ed il polnomio $m(x) = x^2 + x + 2 \in K[x]$. Useremo la norazione $\overline{p(x)}$ per denotare la classe di resto di $p(x)$ modulo $m(x)$. In base alla Proposizione 4.20 per elencare le classi di resto modulo $m(x)$ basta considerare le classi di tutti polinomi scelti tra il polinomio nullo e quelli di grado minore di $2 = \deg m(x)$. Pertanto

$$K[x]/I = \left\{\, \overline{0}, \overline{1}, \overline{2}, \overline{x}, \overline{x+1}, \overline{x+2}, \overline{2x}, \overline{2x+1}, \overline{2x+2} \,\right\}$$

Supponiamo di voler effettuare la moltiplicazione di $(\overline{2x+1})(\overline{x+2}) = \overline{2x^2+2x+2}$ (i coefficienti sono in $\mathbb{Z}_3$). Per determinare quale classe di resto sia $\overline{2x^2+2x+2}$ si può procedere in due modi. Il primo metodo consta nel sostituire a $2x^2 + 2x + 2$ il resto della sua divisione per $m(x)$:

$2x^2$	$+2x$	$+2$	$x^2 + x + 2$
$2x^2$	$+2x$	$+1$	2
		1	

Pertanto $\overline{2x^2+2x+2} = \overline{1}$.

L'altro metotodo consta nel notare che $\overline{m(x)} = \overline{x^2+x+2} = \overline{0}$, quindi $\overline{x^2} = \overline{-x-2}$. Soctituento otteniamo $\overline{2x^2+2x+2} = \overline{2x^2} + \overline{2x+2} = \overline{2(-x-2)} + \overline{2x+2} = \overline{-2} = \overline{1}$.

Proposizione 4.22. *Sia $m(x)$ un polinomio di grado maggiore od eguale a 1 e K un campo allora le seguenti affermazioni sono equivalenti:*

1. *$K[x]/(m(x))$ è un campo,*
2. *$K[x]/(m(x))$ è un dominio,*
3. *$m(x)$ è un polinomio irriducibile.*

Dimostrazione. La dimostrazione è identica a quella della Proposizione 4.4 con l'esclusione del punto *"(3) implica (1)"* che ripetiamo per esteso. Si ponga $I = (m(x))$ e si suponga che $m(x)$ sia irriducibile e che $a(x) + I \neq I$ sia un laterale non nullo. Poiche $m(x)$ non divide $a(x)$ il massimo comun divisore monico $d(x) = h(x)a(x) + k(x)m(x)$ (Teorema di Bezout) tra $a(x)$ e $b(x)$ è uguale a 1 (essendo un divisore del polinomio irriducibile $m(x)$ di grado inferiore al grado di $m(x)$). Pertanto $1 = h(x)a(x)+k(x)m(x) \in h(x)a(x)+I$ cosicché $1 + I = h(x)a(x) + I = (h(x) + I)(a(x) + I)$ e la classe di resto di $h(x)$ è l'inversa della classe di resto di $a(x)$ modulo $m(x)$. □

Notiamo che in $K[x]/I$ le classi di resto $I + c$ dei polinomi costanti $\alpha \in K$ (polinomi di grado 0) formano un sottocampo di $K[x]/I$ isomorfo a K. Cosideriamo infatti l'applicazione $\varphi K \to K[x]/I$ definita da $\alpha \mapsto \alpha + I$. Tale applicazione è un omomorfismo con nucleo uguale a $\{ 0 \}$ e pertanto è iniettiva (questo viene anche dalla Proposizione 4.20). Si conviene allora di identificare K con l'insieme dei laterali della forma $\alpha + I$ al variare di $\alpha \in K$ e di considerare $K[x]/I$ come un anello che contiene K come sottoanello. Scriveremo allora talvolta, con abuso di notazione, α per indicare il laterale $\alpha + I$ di $K[x]/I$. Infine Se $p(x) = a_0 + \cdots + a_m x^m$ è un elemento di $K[x]$ useremo la scrittura $\overline{p(x)}$ per denotare la classe di resto $p(x) + I$ di $p(x)$ modulo $m(x)$. Avremo allora, con la convenzione appena fatta di identificare un elemento α di K con $\overline{\alpha}$, che $\overline{p(x)} = \overline{a_0 + a_1 x + \cdots + a_m x^m} = \overline{a}_0 + \overline{a}_1\overline{x} + \cdots + \overline{a}_m\overline{x}^m = a_0 + a_1\overline{x} + \cdots + a_m\overline{x}^m = p(\overline{x})$. Abbiamo quindi il seguente risultato.

Corollario 4.23. *Con le notazioni di cui sopra, dato un polinomio irriducibile $m(x)$ allora $K[x]/(m(x))$ è un campo che contiene K nel quale $m(x)$ ammette $\overline{x}$ come radice.*

Dimostrazione. Infatti $0 = \overline{0} = \overline{m(x)} = m(\overline{x})$. □

Esempio: costruzione dei numeri complessi. Consideriamo il polinomio $x^2 + 1 \in \mathbb{R}[x]$. Tale polinomio è irriducibile in $\mathbb{R}[x]$ (perché?) e pertanto $F = \mathbb{R}[x]/(x^2 + 1)$ è un campo che contiene $\mathbb{R}$ come sottocampo. Gli elementi di F sono, in virtu della Proposizione 4.20 le classi di resto dei polinomi della forma $a + bx$ al variare id a e b in $\mathbb{R}$. Poiniamo $i = \overline{x}$, avremo $i^2 = \overline{x^2} = \overline{x^2 + 1 - 1} = \overline{x^2 + 1} - \overline{1} = -1$. Gli elementi di F sono pertanto della forma $a + ib$ con $i^2 = -1$ e $a, b \in \mathbb{R}$. Pertanto $F = \mathbb{C}$ è l'insieme dei numeri complessi.

4.3.2 Criteri di irriducibilità

In questo paragrafo diamo alcuni criteri che permettono di stabilire se un polinomio $p(x) \in K[x]$ è irriducibile in dipendenza del campo K. Molti di questi criteri verranno dati senza dimostrazione.

Dal Teorema 4.12 (di Ruffini) si deduce immediatamente che un polinomio in $K[x]$ di grado maggiore od eguale a 2 che ammette una radice $\alpha \in K$ è riducibile in $K[x]$. Non è vero il viceversa: il polinomio $(x^2+1)^2$ è infatti riducibile in $\mathbb{R}[x]$ ma non ha radici in $\mathbb{R}$.

Polinomi irriducibili in $\mathbb{C}[x]$

Teorema 4.24 (Teorema fondamentale dell'algebra)**.** *Ogni polinomio a coefficienti complessi di grado maggiore od eguale ad* 1 *ha almeno una radice in* $\mathbb{C}$*. In paricolare i soli polinomi irriducibili in* $\mathbb{C}[x]$ *sono quelli di primo grado.*

Polinomi irriducibili in $\mathbb{R}[x]$

Poiché $\mathbb{R} \subseteq \mathbb{C}$, un polinomio $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{R}[x]$ di grado $n \geq 2$ ammette almeno una radice $z \in \mathbb{C}$. Se $z \in \mathbb{R}$ allora per il Teorema di Ruffini $p(x)$ è riducibile in $\mathbb{R}[x]$. Se $z \in \mathbb{C} \setminus \mathbb{R}$, usando la notazione di mettere una barra al di sopra di un numero complesso per intenderne il coniugato, troviamo $0 = \overline{0} = \overline{p(z)} = \overline{\sum_{i=0}^{n} a_i z^i} = \sum_{i=0}^{n} \overline{a}_i \overline{z}^i = \sum_{i=0}^{n} a_i \overline{z}^i = p(\overline{z})$. Pertanto $\overline{z}$ è una radice di $p(x)$ diversa da z. Per il toerema di Ruffini si ha che $q(x) = (x-z)(x-\overline{z}) = x^2 - (z+\overline{z})x + z\overline{z} = x^2 - 2\,\mathrm{Re}(z)x + |z|^2 \in \mathbb{R}[x]$ è un divisore di $p(x)$ in $\mathbb{C}[x]$. Pertanto $p(x) = q(x)h(x)$ dove $h(x) \in \mathbb{C}[x]$ è il quoziente della divisione di $p(x)$ per $q(x)$. Poiché i polinomi $p(x)$ e $q(x)$ sono entrambi reali, l'algoritmo della divisione tra polinomi produce un quoziente $h(x)$ a coefficienti reali. Ne consegue che $p(x)$ si fattorizza come prodotto dei due polinomi reali $q(x)$ e $h(x)$ e pertanto $p(x)$ è irriducibile solo se $h(x) = h \in \mathbb{R}$ è una costante non nulla.

Come conseguenza abbiamo il seguente teorema.

Teorema 4.25. *Un polinomio* $p(x) \in R[x]$ *è irriducibile (in* $\mathbb{R}[x]$*) se e solo se vale una delle seguenti condizioni:*

1. $p(x)$ *è un polinomio di primo grado,*
2. $p(x)$ *è un polinomio di secondo grado con una radice non reale (ovvero ha discriminante* $\Delta < 0$*).*

In base al precedente teorema il polinomio $p(x) = x^4 + 1$, pur non avendo radici reali, è riducibile in $\mathbb{R}[x]$ ed è possibile trovarne una fattorizzazione.

Come sopra determiniamo una radice complessa non reale $z = \frac{\sqrt{2}}{2}(1+i)$. Scriviamo $q(x) = (x-z)(x-\overline{z}) = \left(x - \frac{\sqrt{2}}{2}(1+i)\right)\left(x - \frac{\sqrt{2}}{2}(1-i)\right) = x^2 - \sqrt{2}\,x + 1$. Sappiamo che $q(x)$ è un fattore di $p(x)$. A questo punto, dividendo $p(x)$ per $q(x)$, si trova $p(x) = \left(x^2 - \sqrt{2}\,x + 1\right)\left(x^2 + \sqrt{2}\,x + 1\right)$.

Esercizio 4.3. Fattorizzare in $\mathbb{R}[x]$ il polinomio $x^5 - 1$.

Svolgimento: Poniamo $p(x) = x^5 - 1$. Una radice di $p(x)$ è 1, pertanto $p(x) = (x-1)q(x)$ dove $q(x) = x^4 + x^3 + x^2 + x + 1$. Quest'ultimo polinomio, avendo grado 4, non è irriducibile. Le radici di $p(x)$ sono le radici quinte complesse dell'unità:

1. $z_0 = e^{\frac{2\pi}{5}i\cdot 0} = 1$
2. $z_1 = e^{\frac{2\pi}{5}i\cdot 1} = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$
3. $z_2 = e^{\frac{2\pi}{5}i\cdot 2} = \cos\frac{4\pi}{5} + i\sin\frac{4\pi}{5}$
4. $z_3 = e^{\frac{2\pi}{5}i\cdot 3} = \cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$
5. $z_4 = e^{\frac{2\pi}{5}i\cdot 4} = \cos\frac{8\pi}{5} + i\sin\frac{8\pi}{5}$

Posto $\varepsilon = z_1$ si vede facilmente che $z_i = \varepsilon^i$ e che $\overline{z}_j = e^{5-j}$. Pertanto $q(x) = (x-\varepsilon)(x-\varepsilon^2)(x-\varepsilon^3)(x-\varepsilon^4) = \left((x-\varepsilon)(x-\overline{\varepsilon})\right)\left((x-\varepsilon^2)(x-\overline{\varepsilon}^2)\right) = (x^2 - 2\operatorname{Re}\varepsilon + 1)(x^2 - 2\operatorname{Re}\varepsilon^2 + 1)$ è la fattorizzazione di $q(x)$. Non resta che determinare $\operatorname{Re}\varepsilon$ e $\operatorname{Re}\varepsilon^2$. Questo si può fare nel seguente modo. Notiamo che ε è una radice di $q(x)$ e quindi che $0 = \varepsilon^4+\varepsilon^3+\varepsilon^2+\varepsilon+1 = 2\operatorname{Re}\varepsilon + 2\operatorname{Re}\varepsilon^2 + 1$. Tenemdo a mente il fatto che $\varepsilon^5 = 1$ abbiamo anche $(2\operatorname{Re}\varepsilon)(2\operatorname{Re}\varepsilon^2) = (\varepsilon+\varepsilon^4)(\varepsilon^2+\varepsilon^3) = \varepsilon^3 + \varepsilon^4 + \varepsilon + \varepsilon^2 = 2\operatorname{Re}\varepsilon^2 + 2\operatorname{Re}\varepsilon$. I valori di $\alpha = 2\operatorname{Re}\varepsilon$ e $\beta = 2\operatorname{Re}\varepsilon^2$ sono quindi soluzioni del sistema simmetrico:

$$\begin{cases} \alpha + \beta = -1 \\ \alpha\beta = \alpha + \beta \ (= -1) \end{cases}$$

Il problema si riduce a determinare due numeri il cui prodotto è uguale a 1 e la cui somma è uguale a -1 che sono quindi le soluzioni $\alpha = \frac{-1+\sqrt{5}}{2}$ (notando che $\operatorname{Re}\varepsilon > 0$) e $\beta = \frac{-1-\sqrt{5}}{2}$ dell'equazione di secondo grado

$$t^2 + t + 1 = 0$$

Troviamo quindi $\cos\frac{2\pi}{5} = \operatorname{Re}\varepsilon = \alpha/2 == \frac{-1+\sqrt{5}}{4}$ e $\cos\frac{4\pi}{5} = \operatorname{Re}\varepsilon^2 = \beta/2 = \frac{-1-\sqrt{5}}{4}$. *Il lettore è invitato a calocare, usando questi valori, oltre ai*

seni dei detti archi anche i coseni e seni degli archi di $\frac{\pi}{5}$ *e* $\frac{\pi}{10}$. Concludendo la fattorizzazione di $p(x)$ in $\mathbb{R}[x]$ è la seguente

$$x^5 - 1 = (x-1)\left(x^2 + \frac{1-\sqrt{5}}{2}x + 1\right)\left(x^2 + \frac{1+\sqrt{5}}{2}x + 1\right).$$

Polinomi irriducibili in $\mathbb{Q}[x]$

Ogni polinomio non nullo $p(x) \in \mathbb{Q}[x]$ può essere scritto in modo unico nella forma $p(x) = rq(x)$ dove $r \in \mathbb{Q}$ e $q(x)$ ha coefficienti interi, ha coefficiente direttore positivo ed il massimo comun divisore dei coefficienti di $q(x)$ è uno. Illustriamo questo fatto con esempio: $-\frac{35}{12}x^5 + \frac{21}{15}x^3 + 7x + 7 = -\frac{7}{60}(25x^5 - 12x^3 - 60x - 60)$ (si è raccolto a denonimatore il minmo comune multiplo dei denominatori ed al numeratore il massimo comun divisore dei numeratori dei coefficienti del polinomio). Il numero r è detto contenuto di $p(x)$ e $q(x)$ è detta forma primitiva di $p(x)$. Un polinomio in $\mathbb{Q}[x]$ è detto primitivo se coincide coincide con la sua forma primitiva. È anche immediato verificare che *un polinomio in* $\mathbb{Q}[x]$ *è irriducibile se e solo se lo è la sua forma primitiva*. Pertanto ci si può limitare a fornire un criterio che possa stabilire se un polinomio primitivo è irriducibile in $\mathbb{Q}[x]$. Il seguente lemma, che non dimostriamo, ci viene in aiuto a tal fine.

Lemma 4.26 (di Gauss)**.** *Il contenuto e la forma primitiva del prodotto di due polinomi non nulli in* $\mathbb{Q}[x]$ *sono rispettivamente uguali al prodotto dei contenuti ed al prodotto delle forme primitive dei due fattori.*

Proposizione 4.27 (Criterio di Eisenstein)**.** *Sia* $q(x) = \sum_{i=0}^{n} a_i x^i$ *un polinomio non nullo di grado* n *a coefficienti interi e si supponga che esista un numero primo* p *tale che*

1. p *non divide* a_n*,*
2. p *divide* a_i *per* $i \neq n$*,*
3. p^2 *non divide* a_0*.*

Allora $q(x)$ *è irriducibile in* $\mathbb{Q}[x]$*.*

Non è vero il viceversa: ad esempio per il polinomio riducibile $x^2-5x+6 = (x-2)(x-3)$ non esiste alcun primo che soddisfi le tre condizioni del criterio di Eisenstein.

Dimostriamo, come applicazione del criterio di Eisenstein, che. se p è unumero primo allora il polinomio $q(x) = 1 + x + x^2 + \cdots + x^{p-1} = \sum_{i=0}^{p-1} = \frac{x^p-1}{x-1}$

è irriducibile in $\mathbb{Q}[x]$. Calcoliamo $r(t) = q(t+1) = \frac{(t+1)^p - 1}{t} = \sum_{i=1}^{p} \binom{p}{i} t^{i-1} = \binom{p}{1} + \binom{p}{2} t + \cdots \binom{p}{p-1} t^{p-2} + t^{p-1}$. È facile vedere che questo polinomio soddisfa il criterio di Eisenstein relativamente al primo p. Pertanto $r(t)$ è irriducibile. Lasciamo al lettore di dimostrare che $r(t)$ è irriducibile se e solo se $q(x)$ lo è.

4.3.3 Esercizi

Esercizio 4.4. Sia A un anello commutativo ed I e J due ideali di A. Si definisca $IJ = \{ \sum_{s=1}^{n} i_s j_s \mid n \in \mathbb{N}, i_s \in I, j_s \in J \}$. Si dimostri che:

1. IJ e $I \cap J$ sono ideali di A e che $IJ \subseteq (I \cap J)$;
2. Se A è un dominio ad ideali principali e $I = (a)$, $J = (b)$ dove $a, b \in A$, allora $IJ = I \cap J = (d)$, dove d è un massimo comun divisore di a e b.

Esercizio 4.5. Dimostrare che se K è un campo ed $\alpha \in K$ allora l'insieme $I = \{ p(x) \in K[x] \mid p(\alpha) = 0 \}$ è l'ideale (principale) di $K[x]$ generato da $x - \alpha$. Dimostrare che $K[x]/I$ è un anello isomorfo a K (sugg. considerare l'omomorfismo valutazione $\varphi\colon K[x] \to K$ definito da $\varphi(p(x)) = p(\alpha)$ ed usare il Teorema 4.8).

Esercizio 4.6. Si consideri l'anello $A = \mathbb{R}^2$ dove somma e prodotto sono definiti coordinata per coordinata. Si definiscano $I = \{ (a, 0) \mid a \in \mathbb{R} \}$ e $J = \{ (0, b) \mid b \in \mathbb{R} \}$. Dimostrare che $\{ 0 \}$, I, J e A sono tutti e soli gli ideali di A. Generalizzare questo risultato mostrando che $\mathbb{R}^n$ ha esattamente 2^n ideali (uno per ciascun sottoinsieme di $\{ 1, \ldots, n \} \ldots$).

Esercizio 4.7. Siano A e B due anelli commutativi e $f\colon A \to B$ un omomorfismo suriettivo avente nucleo K. Si mostri che se I è un ideale di B allora la sua controimmagine $J = f^{-1}(I)$ è un ideale di A che contiene K. Si mostri anche che l'applicazione Φ che associa ad un ideale di B la sua controimmagine è una biiezione tra l'insieme degli ideali di B e l'insieme degli ideali di A che contengono K, tale biiezione preserva le inclusioni ($\Phi(I) \subseteq \Phi(T)$ se e solo se $I \subseteq T$).

Esercizio 4.8. Per ogni numero intero positivo n determinare esplicitamente in $\mathbb{Q}[x]$ un polinomio irriducibile di grado n.

Indice