ANELLI E MATRICI
MATEMATICA DISCRETA
(CDS I.T.P.S. – TRACK A–L)
A.A. 2023/2024
(VERS. 1.0.3)

VINCENZO C. NARDOZZA

Sommario. In queste note sono presentati i concetti di Teoria degli Anelli incontrati a lezione, disponibili sul testo ufficiale adottato per il corso ma in modo alquanto dispersivo (Capitoli 3, 5 e 8, principalmente; il caso degli anelli polinomiali e degli anelli quoziente, in particolare dei campi finiti, è considerato rispettivamente nei capitoli 6 e 7). Più precisamente sono esposte le proprietà degli anelli $\mathbb{Z}_n$, il Teorema di Eulero–Fermat e la seconda formulazione del Teorema Cinese del Resto; una sezione è dedicata alle proprietà elementari ed essenziali dell'unico anello non commutativo di nostro interesse (anello delle matrici quadrate a coefficienti in un campo), che invece sul libro di testo non è presentato in modo organico. In aggiunta, come utile applicazione della teoria dell'anello delle matrici, è presentato il metodo di eliminazione di Gauss-Jordan per la risoluzione dei sistemi lineari.

Un discreto numero di esercizi (svolti e non) presenti in queste note, assieme a quelli presenti sul libro di testo e nei testi suggeriti (riguardo le matrici) dovrebbero risultare più che sufficienti per assimilare i concetti teorici esposti e raggiungere una adeguata preparazione per la prova scritta.

Indice

1. Anelli

Definizione 1.1. Si dice anello una terna ordinata $(A, *, \circ)$ dove A è un insieme non vuoto, $*$ e $\circ$ sono operazioni binarie interne su A e sono soddisfatti i seguenti assiomi:

(1) $(A, *)$ è un gruppo abeliano;
(2) $(A, \circ)$ è un monoide;
(3) valgono le proprietà *distributive* di $\circ$ rispetto $*$, cioè per ogni $a, b, c \in A$ risulta

$$a \circ (b * c) = (a \circ b) * (a \circ c) \qquad e \qquad (a * b) \circ c = (a \circ c) * (b \circ c).$$

L'anello si dice *commutativo* se in aggiunta $\circ$ soddisfa la proprietà commutativa.

***Esempio* 1.2.** L'*anello degli interi*, cioè la struttura $(\mathbb{Z}, +, \cdot)$, dove con i simboli $+$ e $\cdot$ si denotano le usuali operazioni tra interi, così come le strutture $(\mathbb{Q}, +, \cdot)$ e $(\mathbb{R}, +, \cdot)$ sono anelli commutativi. Di solito ci si riferisce a questi anelli citando il solo insieme ($\mathbb{Z}$, $\mathbb{Q}$ ed $\mathbb{R}$, rispettivamente), perchè si sottintende che le operazioni sono quelle "standard".

Osservazione 1.3. Coerentemente con quanto visto in Teoria dei Gruppi, la prima operazione di un anello si denota con $+$ (essendo commutativa), la struttura $(A, +)$ si dice la *struttura additiva* dell'anello, il relativo elemento neutro si denota con 0_A (molto spesso, direttamente con 0) e si dice *lo zero dell'anello*. La seconda operazione (potenzialmente NON commutativa) si denota invece con $\cdot$, si chiama il *prodotto* dell'anello, il suo elemento neutro si denota con 1_A e si dice l'*unità* dell'anello.

Con questa notazione, le proprietà distributive assumono una forma più usuale:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad e \qquad (a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

E' da sottolineare che, poichè in genere $\cdot$ non è commutativa, entrambe necessitano di una verifica: se vale una sola delle leggi distributive, la struttura NON è un anello.

Come si fa in genere per un prodotto, di solito si scrive direttamente ab per il prodotto $a \cdot b$, sottintendendo il simbolo di moltiplicazione. □

Nel nostro limitato contesto, un anello avrà necessariamente almeno due elementi distinti: 0_A e 1_A.

Osservazione 1.4. C'è una definizione più generale di anello, che non richiede l'esistenza di 1_A, elemento neutro moltiplicativo. Per esempio, mentre per noi la struttura $(2\mathbb{Z}, +, \cdot)$ non è un anello perchè ha unità, in questa definizione più generale essa sarebbe un anello, anche se non unitario. Visto però che gli anelli che considereremo nel nostro corso hanno tutti unità, tanto vale considerare direttamente la richiesta dell'esistenza di 1_A all'interno del sistema di assiomi che definiscono il concetto di anello. Va segnalato, invece, un errore nel libro di testo, e precisamente nella Definizione 8.19, al punto (v): come detto, un anello non è necessariamente commutativo, per cui la richiesta (v) (che è precisamente la proprietà commutativa della moltiplicazione) non dovrebbe essere presente nella lista.

Va osservato che essendo la struttura *anello* una terna ordinata, non è opzionale l'ordine con cui si elencano le operazioni: $(\mathbb{Z}, +, \cdot)$ è un anello, mentre $(\mathbb{Z}, \cdot, +)$ NO, perchè la struttura $(\mathbb{Z}, \cdot)$ non è un gruppo.

Esercizio 1. *Sia X un insieme non vuoto. Decidere se la struttura $(\wp(X), \cup, \cap)$ è un anello. Stessa richiesta per la struttura $(\wp(X), \cap, \cup)$.*

Esercizio 2. *Se X è un insieme non vuoto, e A, B sono suoi sottinsiemi, la loro* differenza simmetrica *è l'insieme $A \triangle B := (A \setminus B) \cup (B \setminus A)$, dove $\setminus$ denota la usuale differenza insiemistica.*

Decidere se la struttura $(\wp(X), \triangle, \cap)$ è un anello.

Esercizio 3. *Se X è un insieme non vuoto, con la notazione dell'esercizio precedente, decidere se $(\wp(X), \triangle, \cup)$ è un anello.*

In quanto elementi neutri per operazioni associative, sappiamo che 0_A e 1_A sono unici. In realtà, 0_A ha una considerevole proprietà anche rispetto il prodotto:

Esercizio 4. *Per ogni $a \in A$ risulta $a0_A = 0_A = 0_A a$; 0_A è l'unico elemento di A con tale proprietà (detta* di assorbimento*).*

***Svolgimento Esercizio* 4.** Poichè 0_A è l'elemento neutro per $+$, si ha $0_A + 0_A = 0_A$. Di conseguenza, se a è un arbitrario elemento di A, risulta $a(0_A + 0_A) = a0_A$. Per una delle proprietà distributive, ciò vuol dire che $a0_A + a0_A = a0_A$ e, poichè $(A, +)$ è un gruppo, da ciò segue che $a0_A = 0_A$. Similmente si ottiene $0_A a = 0_A$.

Sia poi $x \in A$ un elemento con la proprietà che $\forall a \in A$ $ax = x = xa$; ciò deve valere in particolare per $a = 0_A$, per cui deve risultare $0_A x = x$. Ma abbiamo appena provato che $0_A x = 0_A$, per cui $0_A = 0_A x = x$, cioè $x = 0_A$. □

Per questa sua duplice speciale proprietà, l'elemento 0_A gioca un ruolo essenziale tanto per l'addizione quanto per la moltiplicazione di un anello, e viene detto l'elemento *assoluto* dell'anello. Altre proprietà generali di un anello riguardano gli opposti dei suoi elementi, e come interagiscono con la moltiplicazione (ovviamente, con *opposto* dell'elemento $a \in A$ si intende il simmetrico di a rispetto l'operazione $+$, e come per i gruppi additivi esso viene denotato con $-a$).

Esercizio 5. *Per ogni $a, b \in A$, risulta*

$$(-a)b = -(ab) = a(-b).$$

***Svolgimento Esercizio* 5.** Per dimostrare che $(-a)b = -(ab)$, cioè che $(-a)b$ è l'opposto dell'elemento ab, calcoliamo $(-a)b + ab$: per una delle due proprietà distributive, possiamo "mettere in evidenza" b a destra, ottenendo

$$(-a)b + ab = (-a + a)b = 0_A b = 0_A.$$

Poichè $(A, +)$ è un gruppo abeliano, per la commutatività di cui gode l'operazione $+$ e per l'unicità dell'opposto in un gruppo possiamo concludere che $(-a)b$ è l'opposto di ab. La verifica che $a(-b) = -(ab)$ è simile. □

Ovviamente, in un anello è possibile parlare di *multiplo intero* di un suo elemento: se $a \in A$ e $k \in \mathbb{Z}$ l'elemento ka è il multiplo secondo l'intero k dell'elemento a del gruppo abeliano $(A, +)$; allo stesso modo, ha senso parlare di *potenze* di a, purchè con esponente non negativo: essendo $(A, \cdot)$ un monoide, possiamo intendere $a^0 := 1_A$ e, per $k \geqslant 1$, $a^k := a \cdot a \cdot \cdots \cdot a$ (k fattori), ma dato che appunto $(A, \cdot)$ NON è un gruppo, non ha senso parlare di potenze con esponente negativo per un elemento generico di A.

Per l'anello degli interi vale la cosiddetta *legge di annullamento del prodotto*: se $a, b \in \mathbb{Z}$ allora $ab = 0 \Rightarrow a = 0$ oppure $b = 0$. A parole: *un prodotto di interi è nullo*

solo se è nullo almeno uno dei fattori. La stessa cosa vale per gli anelli $\mathbb{Q}$ ed $\mathbb{R}$, ma non è detto che valga per un generico anello A: può ben accadere che ci siano elementi $a, b \in A$, entrambi diversi da 0_A, epperò tali che $ab = 0_A$. Ciò legittima la seguente

Definizione 1.5. Sia A un anello, e a un suo elemento. Se esiste un elemento $b \in A$, $b \neq 0$ tale che $ab = 0_A$, si dice che a è un divisore sinistro di zero, e b un co-divisore destro di zero associato ad a; analogamente, se esiste un elemento $b \in A$, $b \neq 0_A$ tale che $ba = 0_A$, si dice che a è un divisore destro di zero e b un co-divisore sinistro di zero associato ad a. Se $a \neq 0_A$ è un divisore (destro o sinistro) di zero, si dice che a è un divisore *non banale* di zero. L'insieme dei divisori (destri o sinistri) non banali di zero di A si indica con $\mathscr{D}(A)$.

Osservazione 1.6. Certamente 0_A è un divisore di zero, perchè per $1_A \neq 0_A$ risulta ha $1_A 0_A = 0_A = 0_A 1_A$ (e perciò 0_A si dice il divisore banale di zero). Tuttavia, è da tenere presente che in generale se a è un divisore sinistro di zero, cioè se esiste un $b \neq 0_A$ tale che $ab = 0_A$, è tutt'altro che ovvio che $ba = 0_A$: potrebbe facilmente accadere che $ba \neq 0_A$, oppure addirittura che a non sia affatto un divisore destro di zero!

L'insieme dei divisori di zero è l'unione $\{0_A\} \uplus \mathscr{D}(A)$, dove $\uplus$ significa *unione disgiunta*, e costituisce un insieme importante, eventualmente ridotto al solo $\{0_A\}$: ciò accade precisamente se in A vale la legge di annullamento del prodotto, come per gli anelli $\mathbb{Z}$, $\mathbb{Q}$ ed $\mathbb{R}$, e dà luogo alla seguente

Definizione 1.7. Un anello si dice *integro* se $\mathscr{D}(A) = \varnothing$. Un anello commutativo integro si dice un *dominio d'integrità*.

Di conseguenza, gli anelli $\mathbb{Z}$, $\mathbb{Q}$ ed $\mathbb{R}$ sono anelli integri (anzi, un po' di più: sono domini d'integrità).

Oltre ai divisori di zero, in un anello ci sono altri elementi importanti:

Definizione 1.8. Un elemento $u \in A$ si dice *invertibile* se esiste un elemento $v \in A$ tale che $uv = 1_A = vu$. L'insieme degli elementi invertibili di A si denota con $\mathscr{U}(A)$.

Mentre $\mathscr{D}(A)$ può essere vuoto, $\mathscr{U}(A)$ non è mai vuoto: certamente $1_A \in \mathscr{U}(A)$. Chiaro che $0_A \notin \mathscr{U}(A)$: poichè $0_A \neq 1_A$ e per ogni $a \in A$ risulta $a0_A = 0_A = 0_A a$, 0_A non può essere invertibile. Inoltre, a differenza di $\mathscr{D}(A)$, l'insieme $\mathscr{U}(A)$ non è solo un sottinsieme di A, ma eredita dall'anello una struttura forte. Per la precisione, si ha

Esercizio 6. *Per ogni anello A, la struttura $(\mathscr{U}(A), \cdot)$ è un gruppo. Se A è commutativo, $\mathscr{U}(A)$ è un gruppo abeliano.*[1]

Per quanto detto, se $u \in \mathscr{U}(A)$ allora esiste un unico elemento $v \in A$ tale che $uv = 1_A = vu$, che denotiamo direttamente con u^{-1}, e chiamiamo *l'inverso di u*. Si stia bene attenti a non confondere l'opposto di u (che esiste sempre ed è denotato $-u$) con l'inverso di u (che esiste solo se $u \in \mathscr{U}(A)$ ed è denotato con u^{-1}).

Osservazione 1.9. Se $u \in \mathscr{U}(A)$ torna ad aver senso considerarne potenze u^k con esponente k intero (e non solo $\geqslant 0$), perchè appunto a è un elemento del gruppo $(\mathscr{U}(A), \cdot)$ (e quindi non un *generico* elemento di A).

[1] Per la cronaca, ci sono anelli A non commutativi per i quali $\mathscr{U}(A)$ è abeliano.

Quale che sia l'anello A, un elemento $a \in A$ può essere un divisore dello zero, oppure essere invertibile, oppure non essere nè l'una nè l'altra cosa; di certo però non può essere entrambe le cose:

Esercizio 7. *In ogni anello elementi invertibili e divisori di zero formano insiemi disgiunti, cioè se A è un anello allora $\mathscr{U}(A) \cap \mathscr{D}(A) = \varnothing$.*

Svolgimento Esercizio 7. Sia $a \in \mathscr{U}(A)$; se fosse $a \in \mathscr{D}(A)$, per esempio se a fosse un divisore sinistro di zero, e $b \neq 0_A$ un suo codivisore destro di zero, allora da $ab = 0_A$, moltiplicando a sinistra ambo i membri per a^{-1} si avrebbe $a^{-1}(ab) = (a^{-1}a)b = 1_A b = 0_A$, cioè $b = 0_A$, contraddizione. Nel caso in cui a fosse un divisore destro di zero, si ragiona allo stesso modo. □

Sappiamo che negli anelli $\mathbb{Z}, \mathbb{Q}$ ed $\mathbb{R}$ l'insieme dei divisori non banali di zero è vuoto. Per gli elementi invertibili, invece, la situazione è significativamente diversa: i gruppi $\mathscr{U}(\mathbb{Z}), \mathscr{U}(\mathbb{Q})$ e $\mathscr{U}(\mathbb{R})$ sono tutti abeliani, ma mentre $\mathscr{U}(\mathbb{Z}) = \{+1, -1\}$, si ha $\mathscr{U}(\mathbb{Q}) = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ e, similmente, $\mathscr{U}(\mathbb{R}) = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$. In altri termini, in $\mathbb{Z}$ l'insieme degli elementi invertibili è "piccolo" (ha solo due elementi), mentre in $\mathbb{R}$ e $\mathbb{Q}$ è infinito (precisamente, ogni elemento non zero è invertibile). Questa osservazione è la base per una ulteriore distinzione tra anelli commutativi:

Definizione 1.10. Un anello A si dice un *campo* se è commutativo e $\mathscr{U}(A) = A^*$, cioè se è commutativo e ogni elemento non nullo di A è invertibile.

Perciò, $\mathbb{Z}$ è un dominio d'integrità, ma $\mathbb{Q}$ ed $\mathbb{R}$ sono qualcosa di più: sono infatti *campi*. Il seguente esercizio afferma qualcosa di semplice da testare, ma importante da tener presente:

Esercizio 8. *Ogni campo è un dominio d'integrità.*

Ovviamente, il converso è falso: $\mathbb{Z}$ non è un campo. Tuttavia, è interessante osservare che l'essere finito rende equivalenti i due concetti:

Esercizio 9. *Se A è un dominio d'integrità finito $\Rightarrow$ A è un campo.*

Svolgimento Esercizio 9. A è un dominio d'integrità, quindi in particolare è commutativo. Per far vedere che A è un campo, bisogna far vedere che ogni elemento non nullo di A è invertibile. Sia perciò $0 \neq a \in A$, e consideriamo la funzione $\tau : A \to A$ definita da $\tau(x) = ax$ ($= xa$: A è commutativo) per ogni $x \in A$. Allora τ è una funzione iniettiva: per ogni $x, y \in A$, se $\tau(x) = \tau(y)$ allora $ax = ay \Rightarrow a(x - y) = 0$; poichè però A è un dominio d'integrità e $a \neq 0 \Rightarrow x - y = 0$, cioè $x = y$.

A causa della finitezza di A, τ è anche suriettiva, e quindi esiste un $u \in A$ tale che $\tau(u) = 1_A$, cioè $au = 1_A$. Per la commutatività, $ua = 1_A$, e quindi a è invertibile (e $u = \tau^{-1}(1_A)$ ne è l'inverso). Dato che a è arbitrario, ciò vale per ogni $a \in A^*$, cioè $\mathscr{U}(A) = A^*$, e quindi A è un campo. □

Con queste nozioni, in attesa di completare la teoria che ci serve per i nostri (molto limitati) scopi, possiamo già cominciare a studiare una classe di anelli che ci interessa, e fornire ulteriori esempi di anelli.

2. Anello degli interi modulo n e somma diretta di anelli

Sappiamo dalla Teoria dei Gruppi che per ogni $n \geqslant 2$ l'insieme $\mathbb{Z}_n$, munito dell'addizione tra classi di equivalenza, costituisce un gruppo ciclico (e perciò abeliano)

di ordine n, di cui conosciamo tutti i dettagli (generatori ciclici, numero dei sottogruppi, numero di generatori ciclici, numero di elementi di dato periodo). Partendo da ciò possiamo fornire a $(\mathbb{Z}_n, +)$ una seconda operazione ottenendo un anello:

Proposizione 2.1. *Sia $n \geqslant 2$ e sia $\cdot$ l'operazione binaria su $\mathbb{Z}_n$ definita da*

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

per ogni coppia di elementi $[a]_n, [b]_n \in \mathbb{Z}_n$. La struttura $(\mathbb{Z}_n, +, \cdot)$ è un anello commutativo, di cui $[1]_n$ è l'unità.

Dimostrazione. Come per l'addizione tra classi, l'unico punto critico è la verifica che l'operazione $\cdot$ sia *ben definita*: deve risultare cioè vero che se $[a]_n = [a']_n$ e $[b]_n = [b']_n$ allora $[ab]_n = [a'b']_n$ (cioè, che il risultato della moltiplicazione tra classi dipenda effettivamente solo dalle classi, e non dai rappresentanti). Ciò è però immediato, e discende dalla proprietà di compatibilità della congruenza modulo n con la moltiplicazione tra interi. Esplicitamente, per ogni scelta di interi a, a', b, b' tali che $a \equiv a' \pmod{n}$ e $b \equiv b' \pmod{n}$, sappiamo che $ab \equiv a'b' \pmod{n}$. Ciò equivale ad affermare che risulta $[ab]_n = [a'b']_n$, e dunque effettivamente $[a]_n \cdot [b]_n = [a']_n \cdot [b']_n$.

Verificato ciò, il fatto che $(\mathbb{Z}_n, +, \cdot)$ è un anello commutativo con unità $1_{\mathbb{Z}_n} = [1]_n$ costituisce un semplice esercizio di verifica degli assiomi. □

La prima cosa da studiare sono gli insiemi $\mathscr{D}(\mathbb{Z}_n)$ e $\mathscr{U}(\mathbb{Z}_n)$: quali sono, e quanti sono, i loro elementi? La questione è facile da dirimere, grazie alla seguente

Proposizione 2.2. *Sia $n \geqslant 2$. Un elemento $[a]_n$ è invertibile nell'anello $\mathbb{Z}_n$ se e solo se $MCD(a, n) = 1$. In caso contrario, $[a]_n$ è un divisore dello zero.*

Dimostrazione. Sia $a \in \mathbb{Z}$. Dire che $[a]_n \in \mathscr{U}(\mathbb{Z}_n)$ equivale a dire che esiste $[b]_n$ tale che $[a]_n[b]_n = [1]_n$, cioè che esiste un certo intero $b \in \mathbb{Z}$ tale che $ab \equiv 1 \pmod{n}$, il che è equivalente a dire che a ammette un inverso aritmetico modulo n. In altri termini, le affermazioni $[a]_n \in \mathscr{U}(\mathbb{Z}_n)$ e *a ammette un inverso aritmetico modulo n* sono equivalenti. Poichè sappiamo che questa seconda eventualità accade se e solo se $MCD(a, n) = 1$, il primo enunciato del Lemma è provato. In più, sappiamo anche come determinare $[a]_n^{-1}$: basta prendere un inverso aritmetico b di a modulo n, per avere $[a]_n^{-1} = [b]_n$.

Per la seconda parte dell'enunciato, basta osservare che se $[a]_n \notin \mathscr{U}(\mathbb{Z}_n)$ allora (per la prima parte) $d := MCD(a, n) > 1$. Dovendo essere d un divisore di n, in particolare deve risultare $1 < d \leqslant n$. Ora: se $d = n$, vuol dire che $n \mid a$, e quindi $[a]_n = [0]_n$, cioè $[a]_n$ è un divisore di zero in $\mathbb{Z}_n$ (quello banale, $[0]_n$). Perciò, supponiamo che $1 < d < n$. Allora, dalla divisione per d, si ha $a = a'd$ e $n = n'd$, dove $1 < n' < n$. Di conseguenza $[n']_n \neq [0]_n$, e si ha

$$[a]_n[n']_n = [an']_n = [(a'd)n']_n = [a'(dn')]_n = [a']_n[n]_n = [a']_n[0]_n = [0]_n,$$

cioè $[a]_n$ è un divisore non banale di zero in $\mathbb{Z}_n$, e $[n']_n$ ne è un codivisore di zero. In particolare, in questo caso $[a]_n, [n']_n \in \mathscr{D}(\mathbb{Z}_n)$. □

La precedente Proposizione produce varie piacevoli conseguenze:

Corollario 2.3. *Gli elementi invertibili di $\mathbb{Z}_n$ sono tutti e soli i generatori ciclici del gruppo additivo $(\mathbb{Z}_n, +)$. In particolare, $|\mathscr{U}(\mathbb{Z}_n)| = \varphi(n)$.*

Dimostrazione. Per la Proposizione 2.2, $[a]_n \in \mathscr{U}(\mathbb{Z}_n) \iff MCD(a,n) = 1 \iff \langle [a]_n \rangle = \mathbb{Z}_n$. Sappiamo che ci sono esattamente $\varphi(n)$ elementi di periodo (additivo) n in $\mathbb{Z}_n$, per cui quello è anche il numero di elementi invertibili in $\mathbb{Z}_n$. □

Corollario 2.4. $\mathbb{Z}_n = \{[0]_n\} \uplus \mathscr{U}(\mathbb{Z}_n) \uplus \mathscr{D}(\mathbb{Z}_n)$. *In altri termini, in $\mathbb{Z}_n$ ogni elemento non nullo o è invertibile o è un divisore non banale di zero.*

Corollario 2.5. $|\mathscr{D}(\mathbb{Z}_n)| = n - 1 - \varphi(n)$.

E' da sottolineare che in $\mathbb{Z}$, invece, ci sono infiniti elementi non nulli che non sono nè invertibili nè divisori di zero.

Corollario 2.6. $\mathbb{Z}_n$ *è un campo se e solo se n è primo.*

Dimostrazione. $\mathbb{Z}_n$ è un campo $\iff$ ogni elemento non nullo è invertibile. Se n è primo e $[a]_n \neq [0]_n$ allora $MCD(a,n) = 1$, per cui $[a]_n \in \mathscr{U}(\mathbb{Z}_n)$, cioè ogni elemento non nullo di $\mathbb{Z}_n$ è invertibile e quindi $\mathbb{Z}_n$ è un campo. Al contrario, se n non è primo $\Rightarrow$ esiste un divisore $1 < d < n$ di n, per cui $[d]_n \in \mathscr{D}(\mathbb{Z}_n)$ e quindi $\mathbb{Z}_n$ non è un campo. □

Abbiamo così ampliato l'insieme dei campi che possiamo usare nelle applicazioni: ai campi infiniti che conoscevamo ($\mathbb{Q}$ ed $\mathbb{R}$), possiamo aggiungere infiniti esempi di campi finiti: tutti gli $\mathbb{Z}_p$ per p primo positivo. In particolare, $\mathbb{Z}_2$ è il più piccolo esempio di campo: ha solo i due elementi che devono esserci per forza (lo zero e l'unità).

Dalle poche nozioni appena viste consegue con facilità anche un Teorema molto importante, alla base di applicazioni tecnologiche concrete (crittografia a chiave pubblica, si veda la sezione 5.10 del libro di testo):

Corollario 2.7. (Teorema di Eulero–Fermat)
Se a è un intero relativamente primo con n allora $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Dimostrazione. Dire che $MCD(a,n) = 1$ equivale a dire che $[a]_n \in \mathscr{U}(\mathbb{Z}_n)$. Dato che $\mathscr{U}(\mathbb{Z}_n)$ è un gruppo moltiplicativo di ordine $\varphi(n)$, ogni elemento di $\mathscr{U}(\mathbb{Z}_n)$ è periodico di periodo un divisore di $\varphi(n)$, per cui $[a]^{\varphi(n)} = [1]_n$. Tradotto in termini di congruenze, ciò vuol dire che $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Corollario 2.8. (Piccolo Teorema di Fermat)
Sia p un primo; per ogni intero a risulta $a^p \equiv a \pmod{p}$.

Dimostrazione. Dato che p è primo, i soli possibili valori per $MCD(a,p)$ sono 1 oppure p. Se $MCD(a,p) = p$ allora $p \mid a$, e di conseguenza $[a]_p = [0]_p$. In tal caso, è ovvio che $[a]_p^p = [0]_p^p = [0]_p = [a]$, cioè $a^p \equiv a \pmod{p}$. Se invece $MCD(a,p) = 1$ allora per il Teorema di Eulero–Fermat si ha $a^{\varphi(p)} \equiv 1 \pmod{p}$, e poichè p è primo sappiamo calcolare $\varphi(p) = p - 1$. Moltiplicando ambo i membri della congruenza $a^{p-1} \equiv 1 \pmod{p}$ per a si ottiene anche in questo caso che $a^p \equiv a \pmod{p}$. □

I precedenti risultati, in particolare il Teorema di Eulero–Fermat, consentono di effettuare efficacemente la riduzione modulo n della potenza di un intero, sempre che la base della potenza sia relativamente prima con n: per ridurre modulo n (cioè: per calcolare il resto della divisione per n) la potenza a^e del numero a **relativamente primo ad** n basta

- ridurre la base a modulo n;
- ridurre l'esponente e modulo $\varphi(n)$;

- infine, calcolare direttamente il resto della divisione della risultante potenza per n.

Osservazione 2.9. In realtà, si può fare anche meglio di così: sapere che $a^{\varphi(n)} \equiv 1 \pmod{n}$ vuol dire che il periodo di $[a]_n$ come elemento del gruppo moltiplicativo $\mathscr{U}(\mathbb{Z}_n)$ è un divisore d di $\varphi(n)$, non necessariamente $\varphi(n)$. Basta calcolare d controllando i divisori di $\varphi(n)$ e poi ridurre l'esponente non modulo $\varphi(n)$, ma modulo d, risparmiando tempo e calcoli. Ovviamente, non si guadagna nulla se $[a]_n$ ha periodo moltiplicativo proprio $\varphi(n)$; in compenso però si certifica il fatto che $\mathscr{U}(\mathbb{Z}_n)$ è, in questo caso, non solo abeliano ma ciclico, generato da $[a]_n$.

Facciamo qualche esempio:

Esercizio 10. *Determinare $\mathscr{U}(\mathbb{Z}_6)$, $\mathscr{D}(\mathbb{Z}_6)$. Per ciascun elemento invertibile, determinare il suo inverso e il suo periodo moltiplicativo. Per ciascun divisore di zero non banale, determinare i suoi co-divisori di zero.*

***Svolgimento Esercizio* 10.** Sappiamo che $[a]_6 \in \mathscr{U}(\mathbb{Z}_6) \iff MCD(a,6) = 1$, per cui $\mathscr{U}(\mathbb{Z}_6) = \{[1]_6, [5]_6\}$, mentre $\mathscr{D}(\mathbb{Z}_6) = \{[2]_6, [3]_6, [4]_6\}$. Ciascuno degli elementi invertibili coincide con il suo inverso, ma $[1]_6$ ha periodo moltiplicativo 1, mentre $[5]_6$ ha periodo moltiplicativo 2 (e ciò prova anche che $\mathscr{U}(\mathbb{Z}_6)$ è un gruppo ciclico di ordine 2, generato da $[5]_6$).

Per i divisori di zero, sia $[2]_6$ che $[4]_6$ hanno un solo codivisore di zero, $[3]_6$; di conseguenza, i codivisori di zero associati a $[3]_6$ sono invece due. □

Esercizio 11. *Determinare se $[7]_{100}$ e $[12]_{100}$ sono elementi invertibili o divisori di zero in $\mathbb{Z}_{100}$. Nel caso di un elemento invertibile, determinare esplicitamente il suo inverso e il suo periodo moltiplicativo. Nel caso di un divisore di zero, determinare almeno un suo codivisore di zero.*

***Svolgimento Esercizio* 11.** Poichè $MCD(7, 100) = 1$, sappiamo che $[7]_{100} \in \mathscr{U}(\mathbb{Z}_{100})$. Per determinare il suo inverso basta risolvere la congruenza $7x \equiv 1 \pmod{100}$, cioè determinare un inverso aritmetico di 7 modulo 100. Scopriamo facilmente che $x \equiv 43 \pmod{100}$, per cui $[7]_{100}^{-1} = [43]_{100}$.

Dobbiamo ora determinare il periodo moltiplicativo di $[7]_{100}$, cioè il minimo esponente da dare a $[7]_{100}$ per ottenere $[1]_{100}$. Dalla formula per il calcolo di φ conosciamo il valore di $\varphi(100)$: i soli primi che dividono 100 sono 2 e 5, per cui $\varphi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$. Perciò basterà testare come esponenti i soli divisori positivi di $\varphi(100)$, perchè il periodo moltiplicativo di $[7]_{100}$ deve essere uno di essi. Si ha $7^2 = 49$, e $7^4 \equiv 1 \pmod{100}$, per cui il periodo moltiplicativo di $[7]_{100}$ è 4.

Guardiamo ora a $[12]_{100}$: dato che $MCD(12, 100) = 4$, sappiamo che $[12]_{100} \in \mathscr{D}(\mathbb{Z}_{100})$. Per trovare un suo codivisore di zero dobbiamo trovare una classe $[x]_{100}$ tale che il prodotto $12x$ dia un multiplo di 100, cioè determinare una soluzione della congruenza $12x \equiv 0 \pmod{100}$ che non sia già un multiplo di 100, per esempio $x = 25$, per avere il codivisore $[25]_{100}$.

L'esercizio non chiede di farlo, ma possiamo determinare tutti i codivisori di zero associati a $[12]_{100}$: le soluzioni di $12x \equiv 0 \pmod{100}$ sono gli interi $x = 25k$ con $k \in \mathbb{Z}$, per cui i codivisori cercati sono le classi $[25]_{100}$, $[50]_{100}$, $[75]_{100}$. □

Esercizio 12. *Determinare tutte le soluzioni in $\mathbb{Z}_{36}$ dell'equazione $[12]_{36}x = [24]_{36}$.*

***Svolgimento Esercizio* 12.** Una soluzione dell'equazione data deve essere un elemento di $\mathbb{Z}_{36}$, quindi una classe di equivalenza $x = [y]_{36}$ per la quale $[12]_{36}[y]_{36} =$

$[24]_{36}$. Per come è definita la moltiplicazione tra classi, ciò vuol dire che deve risultare $[12y]_{36} = [24]_{36}$, e cioè (traducendo l'uguaglianza tra classi in termini di congruenze) $12y \equiv 24 \pmod{36}$. Questa congruenza è risolubile, equivalente alla congruenza $y \equiv 2 \pmod 3$. L'insieme delle soluzioni intere della congruenza è costituito dai numeri $2 + 3k$ al variare di k in $\mathbb{Z}$, e sappiamo che essi sono ripartiti nelle dodici classi distinte

$$[2]_{36},\ [5]_{36},\ [8]_{36}, [11]_{36},\ [14]_{36},\ [17]_{36},\ [20]_{36},\ [23]_{36},\ [26]_{36},\ [29]_{36},\ [32]_{36},\ [35]_{36}.$$

Ci sono quindi ben dodici soluzioni distinte per l'equazione di primo grado assegnata, non una sola, come ci saremmo forse aspettati! Ciò perchè stiamo risolvendo equazioni non su di un *campo* (come $\mathbb{Q}$ o $\mathbb{R}$), ma su un *anello* in cui ci sono divisori non banali di zero. Più specificamente, nel nostro caso il coefficiente $[12]_{36}$ non è invertibile in $\mathbb{Z}_{36}$, e questo causa la novità.

Ora si dovrebbe anche essere in grado di comprendere bene la seconda parte dell'enunciato della Proposizione 5.8 del libro di testo: la ripartizione delle soluzioni della congruenza in $d = 12$ classi di equivalenza distinte modulo 36 corrisponde al numero di distinte soluzioni dell'equazione data in $\mathbb{Z}_{36}$. □

Esercizio 13. *Calcolare le ultime due cifre del numero* $5607^{38402475948201}$.

***Svolgimento Esercizio* 13.** Sappiamo come procedere: calcolare le ultime due cifre del numero dato vuol dire calcolare il resto della sua divisione per 100, e perciò possiamo ridurre la base modulo 100, ottenendo il numero $7^{38402475948201}$. Poichè $MCD(7, 100) = 1$, in linea di principio possiamo usare il Teorema di Eulero–Fermat per ridurre l'esponente modulo $\varphi(100)$. Tuttavia, in un esercizio precedente abbiamo scoperto che il periodo moltiplicativo di $[7]_{100}$ è 4, e quindi $[7]^4_{100} = [1]_{100}$. Possiamo perciò ridurre direttamente l'esponente modulo 4, ottenendo che il numero dato è congruo a $7^1 = 7$ modulo 100. Perciò, l'ultima cifra del numero dato è 7, e la penultima è 0 (cioè, il numero dato termina con la stringa di cifre decimali 07). □

Esercizio 14. *Calcolare il resto della divisione di* $2^{3394849204839}$ *per* 15.

***Svolgimento Esercizio* 14.** La base della potenza è già ridotta modulo 15, e non possiamo fare altro. Tuttavia, poichè $MCD(2, 15) = 1$, possiamo sfruttare il Teorema di Eulero-Fermat, e ridurre l'esponente modulo $\varphi(15) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$, per cui il numero dato è congruo a 2 elevato al resto della divisione di 3394849204839 per 8, cioè 7. Infatti, dalla divisione col resto si ha che l'esponente è espresso da $q \cdot 8 + 7$, per un certo numero intero q che nemmeno ci interessa indicare esplicitamente. Poichè per il Teorema di Eulero-Fermat risulta $2^8 \equiv 1 \pmod{15}$, si ha

$$2^{3394849204839} = 2^{8q+7} = (2^8)^q 2^7 \equiv 1^q 2^7 = 2^7 \pmod{15}.$$

A questo punto, $2^7 = 128 \equiv 8 \pmod{15}$, per cui il resto cercato è 8.

Avremmo in realtà potuto fare anche un po' meglio: dato che $2^8 \equiv 1 \pmod{15}$ sappiamo che il periodo moltiplicativo di $[2]_{15}$ è al massimo 8, ma può anche essere 2 o 4. In effetti, $2^2 = 4$, ma $2^4 = 16 \equiv 1 \pmod{15}$. Perciò, per una delle proprietà fondamentali del periodo di un elemento periodico, sappiamo che $[2]^{3394849204839}_{15} = [2]^3_{15}$, dato che $3394849204839 \equiv 3 \pmod 4$. Ciò vuol dire che il numero dato è congruo a $2^3 = 8$ modulo 15, e quindi il resto cercato è 8. □

Osservazione 2.10. Il problema di calcolare il resto di $9^{3394849204839}$ diviso per 15 è solo apparentemente simile a quello di prima: poichè $MCD(9, 15) \neq 1$, sarebbe

un errore gravissimo pensare di usare il Teorema di Eulero-Fermat! Come è facile verificare, infatti, $9^{\varphi(15)} = 9^8$ è congruo a 6 modulo 15, e non a 1, come un'inappropriato e malaccorto "utilizzo" del Teorema di Eulero-Fermat sembrerebbe affermare. In effetti, il calcolo del resto cercato è possibile tramite il ricorso al Teorema Cinese del Resto che verrà esposto nella prossima sezione.

Esercizio 15. *Per quali valori di $n \in \mathbb{Z}$ il numero $a_n := 2n^{14} + 5n^{12} + 7n^2 + 4$ è un multiplo di 9?*

***Svolgimento Esercizio* 15.** Se $MCD(n, 9) = 1$ possiamo usare il Teorema di Eulero–Fermat, e poichè $\varphi(9) = 9(1 - \frac{1}{3}) = 9 \cdot \frac{2}{3} = 6$ possiamo concludere che $n^6 \equiv 1 \pmod 9$. Pertanto,

$$a_n \equiv 2n^2 + 5 + 7n^2 + 4 = 9(n^2 + 1) \equiv 0 \pmod 9.$$

Se invece $MCD(n, 9) \neq 1$ allora necessariamente $3 \mid MCD(n, 9)$, e quindi $n^2 \equiv 0 \pmod 9$. In tal caso, $a_n \equiv 4 \pmod 9$ non è un multiplo di 9. La risposta alla domanda è quindi: a_n è un multiplo di 9 se e solo se $MCD(n, 9) = 1$; più esplicitamente, se e solo se n è congruo a $1, 2, 4, 5, 7$ o 8 modulo 9. In realtà, sappiamo anche di più: se $MCD(n, 1) \neq 1$ allora a_n è congruo invariabilmente a 4 modulo 9. □

Possiamo ampliare ulteriormente la lista degli esempi di anelli a disposizione analogamente a quanto fatto per i gruppi: usando gli esempi noti per costruire nuovi anelli, basati sul prodotto cartesiano dei loro insiemi di supporto. Più precisamente, in analogia con quel che avevamo chiamato *prodotto diretto di gruppi*, abbiamo la seguente costruzione:

Proposizione 2.11. *Siano $(A, +_A, \cdot_A)$, $(B, +_B, \cdot_B)$ anelli, e muniamo il prodotto cartesiano $A \times B$ delle operazioni* componente per componente*, definendo cioè per ogni $(a_1, b_1), (a_2, b_2) \in A \times B$*

$$(a_1, b_1) + (a_2, b_2) := (a_1 +_A a_2, b_1 +_B b_2) \qquad (a_1, b_1) \cdot (a_2, b_2) := (a_1 \cdot_A a_2, b_1 \cdot_B b_2).$$

La struttura ottenuta $(A \times B, +, \cdot)$ è un anello, con zero $(0_A, 0_B)$ e unità $(1_A, 1_B)$, denotata con $A \oplus B$ e detta somma diretta degli anelli A e B.

Esercizio 16. *Dimostrare la precedente Proposizione.*

Per anelli stiamo dando preferenza all'espressione *somma diretta* invece che all'espressione *prodotto diretto* usata per i gruppi, e al relativo simbolo $\oplus$ invece che al simbolo $\times$ del prodotto cartesiano, per sottolineare il fatto che la struttura additiva di $A \oplus B$ è il prodotto diretto delle strutture additive degli anelli assegnati, cioè i gruppi $(A, +_A)$ e $(B, +_B)$. La scelta in sè non ha in realtà una grande importanza, e si può usare anche il termine *prodotto diretto* di anelli (e il simbolo $\times$, scrivendo $A \times B$), purchè ciò non crei malintesi. In queste note, comunque, per chiarezza espositiva, ribadiamo che la scelta è del termine *somma* parlando di anelli, e del termine *prodotto* per i gruppi.[2] Inoltre, la definizione di somma diretta di anelli è data solo per due anelli, ma come per i gruppi non c'è alcuna difficoltà ad estenderla

[2]Per dire tutta la verità, l'utilizzo corretto dei termini *somma* e *prodotto* diretto fa riferimento a una questione più sottile e che non è il caso di esporre qui. Per noi, che considereremo solo prodotti cartesiani tra un numero finito di insiemi, la cosa non ha comunque rilevanza e resta una mera questione di scelta di termini

a un numero finito di anelli (le operazioni restano sempre definite *componente per componente*).

Sappiamo che $\mathscr{U}(A\oplus B)$ è un gruppo moltiplicativo, con elemento neutro $1_{A\oplus B} = (1_A, 1_B)$. La descrizione esplicita di questo gruppo discende dal seguente

Esercizio 17. *Sia $(a,b) \in A \oplus B$. Allora (a,b) è invertibile $\iff$ $a \in \mathscr{U}(A)$ e $b \in \mathscr{U}(B)$. In tal caso, $(a,b)^{-1} = (a^{-1}, b^{-1})$.*

Da ciò, si ha subito

Corollario 2.12. *$\mathscr{U}(A \oplus B) = \mathscr{U}(A) \times \mathscr{U}(B)$, cioè il gruppo moltiplicativo degli elementi invertibili di $A \oplus B$ è il prodotto diretto dei gruppi moltiplicativi $\mathscr{U}(A)$ e $\mathscr{U}(B)$.*

Esercizio 18. *Determinare $\mathscr{U}(\mathbb{Z}_2 \oplus \mathbb{Z}_3)$, e i periodi (moltiplicativi) dei suoi elementi. Il gruppo è ciclico?*

***Svolgimento Esercizio* 18.** Sappiamo che $\mathscr{U}(\mathbb{Z}_2) = \{[1]_2\}$ e $\mathscr{U}(\mathbb{Z}_3) = \{[1]_3, [2]_3\}$, perciò $\mathscr{U}(\mathbb{Z}_2 \oplus \mathbb{Z}_3)$ ha esattamente due elementi: $([1]_2, [1]_3)$ e $([1]_2, [2]_3)$. Il primo elemento è $1_{\mathbb{Z}_2\oplus\mathbb{Z}_3}$, e ha periodo 1; il secondo invece ha periodo 2 perchè $([1]_2, [2]_3)^2 = ([1]_2, [4]_3) = ([1]_2, [1]_3)$. Scopriamo così che $\mathscr{U}(\mathbb{Z}_2 \oplus \mathbb{Z}_3)$ è ciclico di ordine 2, generato da $([1]_2, [2]_3)$. □

Esercizio 19. *Determinare $\mathscr{U}(\mathbb{Z}_4 \oplus \mathbb{Z}_3)$, e i periodi (moltiplicativi) dei suoi elementi. Il gruppo è ciclico?*

***Svolgimento Esercizio* 19.** Sappiamo che $\mathscr{U}(\mathbb{Z}_4) = \{[1]_4, [3]_4\}$ e $\mathscr{U}(\mathbb{Z}_3) = \{[1]_3, [2]_3\}$, perciò $\mathscr{U}(\mathbb{Z}_4\oplus\mathbb{Z}_3)$ ha esattamente quattro elementi: $([1]_4, [1]_3)$, $([1]_4, [2]_3)$, $([3]_4, [1]_3)$ e $([3]_4, [2]_3)$. Il primo elemento ha periodo 1, mentre gli altri hanno periodo 2. Perciò $\mathscr{U}(\mathbb{Z}_4 \oplus \mathbb{Z}_3)$ NON è un gruppo ciclico, ma solo un gruppo abeliano di ordine 4. □

Per ciò che riguarda invece i divisori di zero di $A \oplus B$, si ha

Esercizio 20. *Una somma diretta di anelli non è mai un anello integro.*

***Svolgimento Esercizio* 20.** Indipendentemente dal fatto che A e B siano integri o meno, in $A \oplus B$ ci sono almeno gli elementi $(1_A, 0_B)$ e $(0_A, 1_B)$, entrambi non nulli (cioè, diversi da $(0_A, 0_B) = 0_{A\oplus B}$). Per tali elementi si ha $(1_A, 0_B)(0_A, 1_B) = (0_A, 0_B) = 0_{A\oplus B}$, per cui si ha un prodotto nullo tra elementi non nulli, e quindi $A \oplus B$ non è integro. □

In una somma diretta di anelli perciò ci sono un sacco di divisori di zero, perfino se i suoi *addendi diretti* (gli anelli A e B) sono campi. Infine, si ha

Esercizio 21. *Provare che $A \oplus B$ è un anello commutativo se e solo se tali sono sia A che B.*

3. Isomorfismi e il Teorema Cinese del Resto

Definizione 3.1. *(Confrontare con la Definizione 8.22 del libro di testo)*
Siano A, B anelli, e sia $f : A \to B$ una funzione tra gli insiemi A e B. Diciamo che

(1) f è un *omomorfismo di anelli* se preserva entrambe le operazioni; esplicitamente, se per ogni $a_1, a_2 \in A$ risulta

$$f(a_1 +_A a_2) = f(a_1) +_B f(a_2) \qquad \text{e} \qquad f(a_1 \cdot_A a_2) = f(a_1) \cdot_B f(a_2);$$

(2) f è un *isomorfismo di anelli* se è un omomorfismo di anelli, ed è bigettivo;
(3) se esiste un isomorfismo di anelli tra A e B diciamo che A e B sono anelli *isomorfi*, e scriviamo $A \cong B$.

Nella pratica, si snellisce la notazione, scrivendo direttamente $(A, +, \cdot)$ e $(B, +, \cdot)$ invece del più corretto (e più pedante) $(A, +_A, \cdot_A)$ e $(B, +_B, \cdot_B)$, dato che il senso complessivo di una somma o di un prodotto è fornito dal contesto: se troviamo scritto $f(x) + f(y)$, vuol dire che $+ = +_B$, cioè che la somma è effettuata in B.

Esercizio 22. *Sia $f : A \to B$ un omomorfismo di anelli. Provare che*
(1) $f(0_A) = 0_B$*;*
(2) $f(-a) = -f(a)$ *per ogni $a \in A$;*
(3) $f(ka) = kf(a)$ *per ogni $a \in A$ e per ogni $k \in \mathbb{Z}$.*

Se $f : A \to B$ è un omomorfismo di anelli, gli elementi di A che sono mandati in 0_B formano un sottinsieme importante:

Definizione 3.2. Siano A, B anelli, e sia $f : A \to B$ un omomorfismo di anelli. Si dice *nucleo di f* l'insieme

$$\ker(f) := \{a \in A \mid f(a) = 0_B\}.$$

Esercizio 23. *Siano A, B anelli, e sia $f : A \to B$ un omomorfismo di anelli.*
(1) *Provare che $0_A \in \ker(f)$;*
(2) $\ker(f)$ *è un sottogruppo di $(A, +)$;*
(3) *per ogni $x \in \ker(f)$ e per ogni $a \in A$ risulta $ax, xa \in \ker(f)$ (si dice che* $\ker(f)$ assorbe *il prodotto per elementi di A).*

Un segno dell'importanza di questo insieme è fornito dal seguente

Esercizio 24. *Sia $f : A \to B$ un omomorfismo di anelli. Provare che f è iniettivo $\iff \ker(f) = \{0_A\}$. Ciò si esprime a parole dicendo che f* ha nucleo banale.

Manco a dirlo, non ogni funzione tra anelli è un omomorfismo:

Esercizio 25. *Sia $f : \mathbb{Z}_{12} \to \mathbb{Z}_6$ definita da $f([a]_{12}) := [2a]_6$ per ogni $[a]_{12} \in \mathbb{Z}_{12}$. Decidere se f è un omomorfismo di anelli.*

***Svolgimento Esercizio* 25.** Come prima cosa, verifichiamo che f è ben definita, e cioè che se $[a]_{12} = [b]_{12}$ allora $f([a]_{12}) = f([b]_{12})$, cioè che $[2a]_6 = [2b]_6$: se $a \equiv b \pmod{12}$ si ha $12 \mid (a - b)$. Poichè $6 \mid 12$ e $(a - b) \mid 2(a - b)$, per la proprietà transitiva della relazione di divisibilità tra interi risulta che $6 \mid 2(a - b)$, cioè che $2a \equiv 2b \pmod 6$, e f risulta ben definita.

E' poi immediato constatare che f preserva l'addizione: per ogni $[a]_{12}, [b]_{12}$ si ha

$$f([a]_{12} + [b]_{12}) = f([a + b]_{12}) = [2(a + b)]_6 = [2a]_6 + [2b]_6 = f([a]_{12}) + f([b]_{12}).$$

Nonostante ciò, f NON preserva il prodotto: si ha infatti

$$f([4]_{12}^2) = f([4]_{12}) = [8]_6 = [2]_6 \text{ mentre } f([4]_{12}) \cdot f([4]_{12}) = [8]_6 \cdot [8]_6 = [4]_6.$$

Perciò f non è un omomorfismo di anelli. □

Rispetto la struttura moltiplicativa, un *omo*morfismo di anelli si comporta abbastanza bene, ma non benissimo:

Esercizio 26. *Se $f : A \to B$ è un omomorfismo di anelli, allora f preserva le potenze con esponente positivo, cioè $\forall a \in A$ e $\forall n \in \mathbb{N}^*$ risulta $f(a^n) = f(a)^n$.*

D'altra parte, in generale è falso che $f(1_A) = 1_B$, così come è falso che f preservi l'inverso, come il seguente facile esempio mostra:

Esercizio 27. *Verificare che la funzione $f : \mathbb{Z}_{12} \to \mathbb{Z}_6$, definita da $f([a]_{12}) := [4a]_6$ per ogni $[a]_{12} \in \mathbb{Z}_{12}$, è un omomorfismo di anelli, e se ne determini il nucleo. Verificare che f non preserva nè l'unità nè gli inversi.*

Svolgimento Esercizio 27. Dopo aver verificato che f è ben definita (farlo!), si può controllare che f preserva la somma (farlo!). Per il prodotto, se $[a]_{12}, [b]_{12}$ sono arbitrari elementi di $\mathbb{Z}_{12}$ si ha

$$f([a]_{12} \cdot [b]_{12}) = f([ab]_{12}) = [4(ab)]_6 = [16ab]_6 = [4a]_6 \cdot [4b]_6 = f([a]_{12}) \cdot f([b]_{12}).$$

Pertanto, f è un omomorfismo di anelli. Non ci dovrebbero essere particolari problemi nel controllare che $\ker(f) = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\} = \langle [3]_{12} \rangle$, sottogruppo di ordine 4 del gruppo additivo $\mathbb{Z}_{12}$; in particolare, $f(0_{\mathbb{Z}_{12}}) = 0_{\mathbb{Z}_6}$.

D'altro canto, guardando alla parte moltiplicativa della struttura *anello*, si noti che $f(1_{\mathbb{Z}_{12}}) = f([1]_{12}) = [4]_6 \neq [1]_6 = 1_{\mathbb{Z}_6}$: f è un omomorfismo di anelli, e NON preserva l'unità! Così pure, si noti che $[1]_{12} \in \mathscr{U}(\mathbb{Z}_{12})$, ma $f([1]_{12}) = [4]_6 \in \mathscr{D}(\mathbb{Z}_6)$: non solo l'immagine di un elemento invertibile di $\mathbb{Z}_{12}$ non è invertibile, ma addirittura è un divisore non banale di zero in $\mathbb{Z}_6$. La stessa cosa capita per tutti gli altri elementi invertibili di $\mathbb{Z}_{12}$, cioè $[5]_{12}, [7]_{12}$ e $[11]_{12}$.[3] □

Se invece f è un *iso*morfismo, esso preserva tutto quel che c'è da preservare: i due anelli sono rappresentazioni diverse ma perfettamente equivalenti della stessa struttura, e qualunque proprietà sia soddisfatta in uno dei due anelli è riprodotta esattamente nell'altro tramite f. Per esempio, $f(1_A) = 1_B$, un elemento $a \in A$ è invertibile se e solo se $f(a)$ è invertibile in B, e $f(a^{-1}) = f(a)^{-1}$, così come (se $a \in \mathscr{U}(A)$!) per ogni $k \in \mathbb{Z}$ risulta $f(a^k) = f(a)^k$. Infine, la scrittura $A \cong B$ ci dice solo che *esiste* un isomorfismo tra i due anelli, ma non qual è: per dimostrare che gli anelli sono effettivamente isomorfi, bisogna esibire almeno un isomorfismo tra essi. Talvolta ciò sarà evidente, altre volte meno.

Esercizio 28. *Siano A, B anelli. Dimostrare che $A \oplus B \cong B \oplus A$.*

Se f è un isomorfismo, in particolare è una funzione bigettiva per definizione, e quindi ha senso considerarne la funzione inversa $f^{-1} : B \to A$. Essa non è però solo una semplice bigezione: si ha facilmente

Esercizio 29. *Se $f : A \to B$ è un isomorfismo di anelli, allora anche $f^{-1} : B \to A$ è un isomorfismo di anelli.*

Svolgimento Esercizio 29. Intanto, l'esistenza di f^{-1} è garantita perchè f è bigettiva. Proviamo che $\forall b_1, b_2 \in B$ risulta $f^{-1}(b_1 + b_2) = f^{-1}(b_1) + f^{-1}(b_2)$. Posto $a_1 := f^{-1}(b_1)$, $a_2 := f^{-1}(b_2)$, risulta

$$f(a_1 + a_2) \underset{\substack{\uparrow \\ f \text{ hom.}}}{=} f(a_1) + f(a_2) = b_1 + b_2.$$

Perciò $a_1 + a_2$ è la (unica: f è bigettiva!) controimmagine in f di $b_1 + b_2$, cioè $a_1 + a_2 = f^{-1}(b_1 + b_2)$. Da ciò, ricordando chi sono a_1 e a_2, si ottiene $f^{-1}(b_1) + f^{-1}(b_2) = f^{-1}(b_1 + b_2)$, che è quanto volevamo provare.

[3] Va detto che per evitare questi (e altri) inconvenienti, spesso la definizione di omomorfismo tra anelli con unità richiede esplicitamente che sia soddisfatta l'extra condizione $f(1_A) = 1_B$, diversamente dalla Definizione 8.22 del libro di testo (che è poi la definizione da noi adottata).

In modo del tutto analogo si può verificare che $f^{-1}(b_1b_2) = f^{-1}(b_1)f^{-1}(b_2)$. Quindi anche f^{-1} è un omomorfismo. □

Un esempio importante di omomorfismo, non iniettivo ma suriettivo, è costituito dalla "solita" proiezione canonica $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$, il che spiega perchè gli anelli $\mathbb{Z}_n$ conservino alcune delle proprietà dell'anello $\mathbb{Z}$ (essere commutativi, per esempio) ma non altre (per esempio, mentre $\mathbb{Z}$ è un dominio d'integrità ma non un campo, per gli $\mathbb{Z}_n$ o si ha un campo, o non si ha nemmeno un dominio d'integrità!):

Esercizio 30. *Dimostrare che per ogni $n \geqslant 2$ la funzione $\pi_n : \mathbb{Z} \to \mathbb{Z}_n$, definita ponendo $\pi_n(k) := [k]_n$ per ogni $k \in \mathbb{Z}$, è un omomorfismo suriettivo di anelli, e preserva l'unità dell'anello.*

Più in generale, si ha

Esercizio 31. *Sia $f : A \to B$ un omomorfismo di anelli. Se f è suriettivo allora $f(1_A) = 1_B$.*

Con le nuove conoscenze, possiamo riformulare il Teorema Cinese del Resto ottenendone una versione equivalente ma molto più efficace nelle applicazioni:

Teorema 3.3. (Seconda formulazione del Teorema Cinese del Resto) *Siano $m, n \geqslant 2$. Se $MCD(m, n) = 1$ allora la funzione*

$$\begin{array}{rccc} \gamma : & \mathbb{Z}_{mn} & \to & \mathbb{Z}_m \oplus \mathbb{Z}_n \\ & [a]_{mn} & \to & ([a]_m, [a]_n) \end{array}$$

è un isomorfismo di anelli.

Dimostrazione. La prima cosa da verificare è che γ sia ben definita, e cioè che per ogni $a, b \in \mathbb{Z}$ se $[a]_{mn} = [b]_{mn}$ allora $([a]_m, [a]_n) = ([b]_m, [b]_n)$: se infatti $a \equiv b \pmod{mn}$ allora $(mn) \mid (a - b)$ e dato che mn è un multiplo tanto di m quanto di n, per la proprietà transitiva della relazione di divisibilità segue che $a - b$ è a sua volta un multiplo tanto di m quanto di n, cioè $a \equiv b \pmod{m}$ e $a \equiv b \pmod{n}$. Tradotto in termini di classi di equivalenze, si ha che sono vere sia l'uguaglianza $[a]_m = [b]_m$ che l'uguaglianza $[a]_n = [b]_n$, e quindi le coppie ordinate $\gamma([a]_{mn})$ e $\gamma([b]_{mn})$ sono uguali. Ciò prova che γ è ben definita.

La verifica che γ è un omomorfismo di anelli, cioè che preserva sia la somma che il prodotto è elementare, e lasciata al lettore. Fatto ciò, sappiamo che γ è un omomorfismo di anelli, e resta da provare solo che γ è bigettiva.

Proviamo l'iniettività: poichè già sappiamo che γ è un omomorfismo, basta provare che il nucleo è banale. Perciò, supponiamo che $[a]_{mn} \in \ker(\gamma)$ e proviamo che allora $[a]_{mn} = [0]_{mn}$. Difatti, dire che $[a]_{mn} \in \ker(\gamma)$ vuol dire che $\gamma([a]_{mn}) = ([0]_m, [0]_n)$, cioè che $a \equiv 0 \pmod{m}$ e $a \equiv 0 \pmod{n}$. Da ciò segue che a è un multiplo comune a m ed n, e quindi è un multiplo di $mcm(m, n)$ per definizione di *minimo comune multiplo tra m ed n*. D'altra parte, poichè $MCD(m, n) = 1 \Rightarrow mcm(m, n) = mn$, e quindi a è un multiplo di mn, cioè $(mn) \mid a$. In termini di classi di equivalenza, ciò vuol dire $[a]_{mn} = [0]_{mn}$.

Avendo provato che il nucleo è banale, sappiamo che γ è iniettiva. Inoltre, poichè $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \oplus \mathbb{Z}_n$ sono insiemi finiti e con la stessa cardinalità $\Rightarrow \gamma$ è necessariamente anche suriettiva, e quindi è non solo un *omo*morfismo, ma un *iso*morfismo di anelli. □

Questa e la prima formulazione del TCR sono equivalenti: nella prima formulazione sostanzialmente provavamo che la funzione γ è suriettiva, da cui discende che γ è anche iniettiva. Qui, abbiamo provato la suriettività passando invece per l'iniettività. In più, però, in questa formulazione abbiamo l'importante informazione che γ è non solo una bigezione, ma un isomorfismo di anelli, e ciò ha conseguenze molto profonde.

Esercizio 32. *Calcolare il resto della divisione di* $15^{748374949292}$ *per* 21.

***Svolgimento Esercizio* 32.** Non possiamo usare il Teorema di Eulero-Fermat per ridurre l'esponente: $MCD(15,21) = 3 \neq 1$. Però possiamo usare l'isomorfismo del TCR per lavorare in $\mathbb{Z}_3 \oplus \mathbb{Z}_7$ invece che in $\mathbb{Z}_{21}$: infatti detto r il resto cercato, poichè deve essere $[r]_{21} = [15]_{21}^{748374949292}$ e la funzione γ è un isomorfismo di anelli, deve risultare $\gamma([r]_{21}) = ([15]_3, [15]_7)^{748374949292}$, cioè

$$\begin{cases} r \equiv 15^{748374949292} \pmod 3 \\ r \equiv 15^{748374949292} \pmod 7 \end{cases} \iff \begin{cases} r \equiv 0 \pmod 3 \\ r \equiv 1 \pmod 7 \end{cases}.$$

Risolvendo il sistema (cioè: tornando a lavorare in $\mathbb{Z}_{21}$ tramite γ^{-1}) si ottiene $r \equiv 15 \pmod{21}$, che è il resto voluto. □

Esercizio 33. *Determinare per quali interi* $n \in \mathbb{Z}$ *il numero*

$$a_n := n^{95} + 23n^{69} - 31n^{51} + 67n^{13}$$

è un multiplo di 30.

***Svolgimento Esercizio* 33.** Poichè $30 = 6 \cdot 5$, e $MCD(5,6) = 1$, per il TCR è $\mathbb{Z}_{30} \cong \mathbb{Z}_6 \oplus \mathbb{Z}_5$. Poichè inoltre $6 = 2 \cdot 3$ e $MCD(2,3) = 1$, è $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$, e quindi $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$. Non c'è alcun problema a costruire un esplicito isomorfismo di anelli: basta considerare la funzione γ definita da $\gamma([a]_{30}) := ([a]_2, [a]_3, [a]_5)$ per ogni $[a]_{30} \in \mathbb{Z}_{30}$ (una terna ordinata, invece che una coppia). Dopodichè, dire che per ogni $n \in \mathbb{Z}$ risulta $[a_n]_{30} = [0]_{30}$ (cioè: ogni a_n è un multiplo di 30) è equivalente a dire che $([a_n]_2, [a_n]_3, [a_n]_5) = ([0]_2, [0]_3, [0]_5)$ per ogni $n \in \mathbb{Z}$. Perciò invece che ragionare in $\mathbb{Z}_{30}$ ragioniamo "parallelamente" ma separatamente in $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$.
Ragioniamo in $\mathbb{Z}_2$: abbiamo due soli casi da discutere, precisamente ciò che accade se $2 \mid n$ e quel che accade se $2 \nmid n$. Se $2 \mid n$ allora $n \equiv 0 \pmod 2$, e di conseguenza $a_n \equiv 0 \pmod 2$. Se invece $2 \nmid n$ allora $MCD(n,2) = 1$ (perchè 2 è primo!) e possiamo usare il Teorema di Eulero-Fermat, deducendo che $n \equiv 1 \pmod 2$. In tal caso, $a_n \equiv 1+1+1+1 \equiv 0 \pmod 2$, cioè $a_n \equiv 0 \pmod 2$. In ambo i casi, abbiamo che $a_n \equiv 0 \pmod 2$, e dunque $[a_n]_2 = [0]_2$ per ogni $n \in \mathbb{Z}$.
Ragioniamo in $\mathbb{Z}_3$: Similmente a quanto fatto per 2, se $3 \mid n \Rightarrow a_n \equiv 0 \pmod 3$, per cui supponiamo $3 \nmid n$. Allora $MCD(n,3) = 1 \Rightarrow n^2 \equiv 1 \pmod 3$ per il Teorema di Eulero-Fermat e si ha $a_n \equiv n + 2n - n + n \equiv 0 \pmod 3$. Perciò $a_n \equiv 0 \pmod 3$ per ogni $n \in \mathbb{Z}$.
Ragioniamo in $\mathbb{Z}_5$: Se $5 \mid n \Rightarrow a_n \equiv 0 \pmod 5$. Perciò supponiamo $5 \nmid n$. Allora $MCD(n,5) = 1 \Rightarrow n^4 \equiv 1 \pmod 5$, e si ha $a_n \equiv n^3 + 3n - n^3 + 2n \equiv 0 \pmod 5$. In definitiva, $a_n \equiv 0 \pmod 5$ per ogni $n \in \mathbb{Z}$.
Pertanto, per ogni $n \in \mathbb{Z}$ risulta $\gamma([a_n]_{30}) = ([0]_2, [0]_3, [0]_5)$. Poichè γ è un isomorfismo, segue che $a_n \equiv 0 \pmod{30}$ per ogni $n \in \mathbb{Z}$. □

Esercizio 34. *Calcolare il resto della divisione di* $9^{23248295834}$ *per* 21.

Svolgimento Esercizio 34. Poichè $\mathbb{Z}_{21} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_7$, possiamo lavorare in parallelo modulo 3 e modulo 7, invece che modulo 21. Il resto r cercato dovrà perciò soddisfare il sistema

$$\begin{cases} r \equiv 9^{23248295834} \pmod 3 \\ r \equiv 9^{23248295834} \pmod 7 \end{cases}.$$

La prima congruenza è di facile riscrittura: $r \equiv 0 \pmod 3$. Per la seconda congruenza, possiamo ridurre $9 \equiv 2 \pmod 7$, e sappiamo che $2^3 \equiv 1 \pmod 7$ (cioè il periodo moltiplicativo di $[2]_7$ è 3), per cui possiamo ridurre l'esponente modulo 3 ottenendo 2, e quindi $r \equiv 2^2 = 4 \pmod 7$. Perciò, il sistema è equivalente a

$$\begin{cases} r \equiv 0 \pmod 3 \\ r \equiv 4 \pmod 7 \end{cases},$$

che ha come soluzioni intere $r = 18 + 21k$ per ogni $k \in \mathbb{Z}$. In altri termini, il resto cercato è 18. □

Osservazione 3.4. L'idea di chiamare *calcolo parallelo* ciò che facciamo passando da $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \oplus \mathbb{Z}_n$ è presente nel libro di testo, si veda a pagina 127. Il TCR, nella forma proposta e dimostrato in queste note, è presente nel libro di testo come Proposizione 5.9 e come Esercizio 27 del Capitolo 5. Nel testo di riferimento, però, manca la verifica che la funzione γ (nel libro di testo indicata con f) sia effettivamente ben definita.

Fatti questi esempi sull'utilizzo del Teorema Cinese dei Resti nella sua seconda formulazione, possiamo usarlo per calcolare effettivamente i valori della funzione di Eulero: già sappiamo che $\varphi(p) = p - 1$ per ogni primo p. Per una potenza di p si ha poi

Proposizione 3.5. *Per ogni primo p e ogni intero $e \geqslant 1$ risulta $\varphi(p^e) = p^e \left(1 - \frac{1}{p}\right)$.*

Dimostrazione. $\varphi(p^e) = |\mathscr{U}(\mathbb{Z}_{p^e})| = |U(p^e)|$, cioè il numero di interi $0 < k \leqslant p^e$ tali che $MCD(k, p^e) = 1$. Invece di contare direttamente quanti sono, contiamo quanti sono quelli per i quali $MCD(k, p^e) > 1$. Notiamo come prima cosa che poichè p è primo, dire che $MCD(k, p^e) > 1$ equivale a dire che $p \mid k$, cioè se k è un multiplo di p. In tal caso, $k = pq$ per un opportuno q, e dato che $0 < k = pq \leqslant p^e \Rightarrow 0 < q \leqslant p^{e-1}$. Ci sono perciò esattamente p^{e-1} scelte per q, e quindi ci sono esattamente p^{e-1} multipli di p nel range $0 < k \leqslant p^e$. Dato che in tutto ci sono p^e numeri in quel range, quelli che sono coprimi con p^e sono esattamente $p^e - p^{e-1} = p^e(1 - \frac{1}{p})$. □

Possiamo ora dimostrare la formula già enunciata a suo tempo per il calcolo di $\varphi(n)$:

Teorema 3.6. *Per ogni intero $n \geqslant 2$ si ha*

$$\varphi(n) = n \prod_{\substack{p \text{ primo} \\ p \mid n}} \left(1 - \frac{1}{p}\right).$$

Dimostrazione. Siano $p_1, \ldots, p_k$ i primi positivi distinti che dividono n, per cui la fattorizzazione di n risulta $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ con esponenti $e_i \geqslant 1$ per ogni $i = 1, \ldots, k$. A causa del TCR, si ha l'isomorfismo di anelli $\gamma : \mathbb{Z}_n \to \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$. Poichè γ è un isomorfismo, si ha che

$$u \in \mathscr{U}(\mathbb{Z}_n) \quad \iff \quad \gamma(u) \in \mathscr{U}\left(\mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{e_k}}\right) = \mathscr{U}(\mathbb{Z}_{p_1^{e_1}}) \times \cdots \times \mathscr{U}(\mathbb{Z}_{p_k^{e_k}})$$

(si riguardi l'Esercizio 17 e il successivo Corollario). Poichè un isomorfismo in particolare è bigettivo, e $|\mathscr{U}(\mathbb{Z}_m)| = \varphi(m)$ per ogni $m \in \mathbb{N}$, si ha di conseguenza

$$\varphi(n) = \varphi(p_1^{e_1})\varphi(p_2^{e_2}) \dots \varphi(p_k^{e_k}).$$

Dalla Proposizione precedente sappiamo che $\varphi(p^e) = p^e \left(1 - \frac{1}{p}\right)$, per cui

$$\begin{aligned}\varphi(n) &= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) p_2^{e_2}\left(1 - \frac{1}{p_2}\right) \dots p_k^{e_k}\left(1 - \frac{1}{p_k}\right) \\ &= p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)\end{aligned}$$

e il prodotto dei fattori in parentesi è precisamente quello delle espressioni $1 - \frac{1}{p}$ al variare di p fra tutti e soli i primi positivi che dividono n. □

Esercizio 35. *Calcolare $\varphi(10000)$, $\varphi(35)$, $\varphi(99)$.*

Svolgimento Esercizio 35. Facile: i soli primi che dividono 10000 sono 2 e 5, perciò

$$\varphi(10000) = 10000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4000.$$

Allo stesso modo basta sapere che i soli primi che dividono 35 sono 5 e 7 per calcolare $\varphi(35) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$ e similmente $\varphi(99) = 99 \cdot \frac{2}{3} \cdot \frac{10}{11} = 60$. □

Dalla dimostrazione del precedente risultato (o se vogliamo, dal TCR) segue anche il seguente

Corollario 3.7. ***(Moltiplicatività della φ di Eulero)***
Se m, n sono interi coprimi $\geqslant 2$ si ha $\varphi(mn) = \varphi(m)\varphi(n)$.[4]

Esercizio 36. *Provare che $[4]_{105} \in \mathscr{U}(\mathbb{Z}_{105})$ e determinarne i periodi additivo e moltiplicativo.*

Svolgimento Esercizio 36. Poichè $MCD(4, 105) = 1$ si ha che $[a]_{105}$ è invertibile in $\mathbb{Z}_{105}$, ed essendo un generatore ciclico del gruppo $(\mathbb{Z}_{105}, +)$ ovviamente il suo periodo additivo è 105. Cioè, 105 è il minimo intero positivo tale che $k[4]_{105} = [0]_{105}$.

Veniamo al calcolo del periodo moltiplicativo m di $[4]_{105}$: poichè $2 \nmid 105$, i numeri 4 e 105 sono coprimi, per cui possiamo utilizzare il Teorema di Eulero–Fermat per concludere che $m \mid \varphi(105)$. Sappiamo calcolare $\varphi(105)$: poichè $105 = 3 \cdot 5 \cdot 7$, si ha

$$\varphi(105) = 105 \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{6}{7} = 48,$$

e quindi m è uno dei 10 divisori positivi di 48: $1, 2, 3, 4, 6, 8, 12, 16, 24$ e 48. Possiamo testarli tutti e scoprire quale è il minimo tra essi che dia $4^k \equiv 1 \pmod{105}$. Per esempio, chiaro che m non può essere 1, 2 o 3 (perchè $1 < 4^k < 105$ per ciascuno di essi), dopodichè $4^4 = 256 \equiv 46 \pmod{105}$ e quindi possiamo scartare 4; poi $4^6 = 4^4 \cdot 4^2 \equiv 46 \cdot 16 = 736 \equiv 1 \pmod{105}$, e quindi concludere che $m = 6$. □

Esercizio 37. *Provare che $[128]_{225} \in \mathscr{U}(\mathbb{Z}_{225})$ e determinarne il periodo moltiplicativo.*

[4] Nel libro di testo, questa proprietà è enunciata a pag. 132, dopo la Definizione 5.3, e per la dimostrazione si è rimandati all'Esercizio 34 di pag. 134.

Svolgimento Esercizio 37. E' chiaro che $MCD(128, 225) = 1$, per cui $[128]_{225} \in \mathscr{U}(\mathbb{Z}_{225})$ e resta da calcolarne solo il periodo moltiplicativo: per il Teorema di Eulero–Fermat, esso deve essere un divisore m di $\varphi(225) = 120$, solo che stavolta i divisori da testare sono 16, e precisamente

$$1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120,$$

un po' troppi e un po' troppo grossi da dare come esponente a 128, anche perchè potremmo non essere fortunati come nell'esercizio di prima e ottenere $m = 120$.

Possiamo aggirare l'ostacolo usando il TCR, lavorando in $\mathbb{Z}_9 \oplus \mathbb{Z}_{25}$ invece che in $\mathbb{Z}_{225}$. Allora si tratta di calcolare il periodo dell'elemento $\gamma([128]_{225}) = ([128]_9, [128]_{25}) = ([2]_9, [3]_{25})$, e precisamente determinare il minimo intero positivo k tale che

$$\begin{cases} 2^k \equiv 1 \pmod 9 \\ 3^k \equiv 1 \pmod{25} \end{cases}.$$

Poichè $\varphi(9) = 6$, il periodo (moltiplicativo) di $[2]_9$ è un divisore di 6, cioè $1, 2, 3$ o 6. Poichè $2^3 = 8$, esso dev'essere 6, e quindi affinchè $2^k \equiv 1 \pmod 9$ dev'essere $6 \mid k$. Cioè, m dev'essere un multiplo di 6. Ragionando alla stessa maniera, dato che $\varphi(25) = 20$, il periodo moltiplicativo di $[3]_{25}$ dev'essere un divisore di 20 cioè $1, 2, 4, 5, 10$ o 20. Si vede subito che non è nè 1, nè 2 nè 3; poi $3^4 = 81 \cong 6 \pmod{25}$, $3^5 = 3^4 \cdot 3 \equiv 6 \cdot 3 = 18 \pmod{25}$, e $3^{10} \equiv 18^2 = 324 \equiv -1 \pmod{25}$, per cui il periodo moltiplicativo di $[3]_{25}$ è 20, e dato che 3^m deve essere congruo a 1 modulo $25 \Rightarrow m$ è anche un multiplo di 20.

Allora basta prendere $m := mcm(6, 20) = 60$: tale valore è il minimo esponente da dare a $([2]_9, [3]_{25})$ per avere $([1]_9, [1]_{25})$. Dato che γ è un isomorfismo, e $([2]_9, [3]_{25}) = \gamma([128]_{225}) \Rightarrow$ il periodo moltiplicativo di $[128]_{225}$ è 60. □

4. Polinomi e anelli quoziente

Una classe di anelli commutativi centrale in tutte le questioni è quella costituita dai polinomi a coefficienti in un anello commutativo. In realtà, nel nostro corso consideriamo solo quelli a coefficienti in un campo (e non nella piena generalità). In questa maniera tutte le proprietà principali cui siamo abituati con i polinomi a coefficienti in $\mathbb{Q}$ o in $\mathbb{R}$ si conservano. Tra esse, di particolare importanza sono

- il grado del prodotto di due polinomi non nulli è la somma dei gradi dei fattori;
- i polinomi a coefficienti in un campo costituiscono un dominio d'integrità;
- vale il Lemma sulla divisione euclidea tra polinomi
- esiste il MCD tra polinomi, ed è ottenibile tramite l'algoritmo euclideo
- i concetti di *primo* e *irriducibile* restano concetti logicamente equivalenti
- vale il Teorema di fattorizzazione unica.

La trattazione dei polinomi è svolta dettagliatamente nel libro di testo, precisamente nel capitolo 6. Più specificamente, sono stati considerati i contenuti dei paragrafi 1, 2 e 3. Le sezioni 4, 5 (circa la questione dell'irriducibilità di polinomi a coefficienti razionali), 6, 7, 8 e 9 (circa il calcolo della complessità computazionale) non sono parte del programma svolto a lezione.

La naturale estensione della congruenza modulo un intero alla congruenza modulo un polinomio, e la costruzione dei relativi anelli quozienti e di nuovi campi (in particolare, di campi finiti di ordine la potenza di un primo) è trattata estesamente nel capitolo 7 del testo adottato, ed è parte effettiva del programma del corso.

Alla luce di ciò, e fatte le precedenti specifiche, non si ritiene utile inserire in queste note ulteriori considerazioni su anelli di polinomi e loro quozienti, rimandando lo studente agli specifici contenuti sul testo adottato.

Si ritiene, invece, utile inserire qualche esercizio svolto in cui sono considerati anelli $\mathbb{Z}_p[x]$, per p primo.

Esercizio 38. *Determinare i polinomi irriducibili di grado* $\leqslant 3$ *di* $\mathbb{Z}_2[x]$.

***Svolgimento Esercizio* 38.** Sono chiaramente irriducibili i due polinomi $x, x+1 \in \mathbb{Z}_2[x]$ (dove scriviamo 0 invece che $[0]_2$ e 1 invece che $[1]_2$ per semplificare la notazione). Ci sono poi quattro polinomi di grado due: x^2, x^2+1, x^2+x e x^2+x+1. I primi tre però sono riducibili:

$$x^2 = x \cdot x, \quad x^2+1 = (x+1)^2 \quad x^2+x = x(x+1).$$

Il polinomio x^2+x+1 è invece irriducibile: è un polinomio di grado 2, e non ha radici in $\mathbb{Z}_2 \Rightarrow$ è irriducibile a causa del Teorema di Ruffini. Infatti se fosse riducibile sarebbe prodotto di due polinomi di grado 1, e di conseguenza dovrebbe avere una radice in $\mathbb{Z}_2$. Questo quindi è l'unico polinomio irriducibile di grado 2 in $\mathbb{Z}_2[x]$.

Anche per i polinomi di grado 3 possiamo usare il Teorema di Ruffini: basta prendere i polinomi di terzo grado che non hanno radici in $\mathbb{Z}_2$. Dato che un generico polinomio di terzo grado è del tipo x^3+bx^2+cx+d, ed è chiaramente riducibile se $d=0$ (è un multiplo di x), basta cercare tra i polinomi x^3+ax^2+bx+1 quelli che non hanno radici in $\mathbb{Z}_2$. Nessuno di essi ha 0 come radice, per cui basta valutare cosa accade per $x=1 \in \mathbb{Z}_2$: si ha $f(1) = 1+a+b+1 = a+b$, e vale zero $\iff$ $a+b=0$, cioè per x^3+x^2+x+1 e x^3+1. Quindi questi due polinomi sono riducibili in $\mathbb{Z}_2[x]$, mentre gli altri due polinomi x^3+x^2+1 e x^3+x+1 sono gli unici due polinomi irriducibili di terzo grado in $\mathbb{Z}_2[x]$. □

Esercizio 39. *Calcolare quoziente e resto della divisione* $(3x^3+2x^2-x-1) : (2x+1)$ *in* $\mathbb{Z}_5[x]$.

***Svolgimento Esercizio* 39.** L'unico possibile problema risiede nel computo dei coefficienti del quoziente: al primo passo, bisogna cercare qual è il monomio w tale che $(2x)w = 3x^3$. E' chiaro che la parte letterale deve essere x^2, ma con quale coefficiente? Se $w = \alpha x^2$ per un certo $\alpha \in \mathbb{Z}_5$ tale che $2\alpha = 3$, dev'essere $\alpha = 2^{-1} \cdot 3$, cioè 3 per l'inverso di 2 in $\mathbb{Z}_5$ (notazione semplificata: ricordiamo che con 2 in realtà stiamo intendendo $[2]_5 \in \mathbb{Z}_5$!), che è 3 (cioè: $[3]_5 \in \mathbb{Z}_5$). Quindi $\alpha = 3 \cdot 3 = 9 = 4$ (ricordiamo ancora una volta, e poi basta, che lavoriamo in $\mathbb{Z}_5$: scriviamo degli interi, ma intendiamo le loro classi di congruenza modulo 5). In effetti, $(2x)(4x^2) = 8x^3 = 3x^3$.

Fatto ciò, qui e nelle successive divisioni, si ottiene che $3x^3+2x^2-x-1 = (2x+1)(4x^2+4x)+1$, per cui il quoziente è $4x^2+4x$, e il resto è 1. □

Esercizio 40. *Calcolare il MCD tra i polinomi* $f = x^3-2x+2$ *e* $g = 2x^2-1$ *di* $\mathbb{Z}_5[x]$*, ed esprimerlo nella sua forma di Bezout.*

***Svolgimento Esercizio* 40.** Usando l'algoritmo euclideo, calcoliamo

$$f = 3xg + (x+2)$$
$$g = (2x-4)(x+2) + 2.$$

Da ciò sappiamo che il polinomio (costante) $m=2$ è un massimo comun divisore tra f e g, ma non è il massimo comun divisore tra f e g perchè NON è monico. Pertanto,

$MCD(f,g)$ è l'unico associato di m monico, cioè 1, che si ottiene moltiplicando $m=2$ per l'inverso del suo coefficiente direttore (sempre 2), cioè per 3.

Fatto ciò, conosciamo anche una coppia di coefficienti di Bezout per $1=MCD(f,g)$: codificando al solito $f \leftrightsquigarrow (1,0)$, $g \leftrightsquigarrow (0,1)$ da $x+2=f-3x\cdot g$ si ha anche $x+2 \leftrightsquigarrow (1,0)-3x\cdot(0,1)=(1,-3x)$. Dopodichè, da $2=g-(2x-4)(x+2)$ si ha anche $2 \leftrightsquigarrow (0,1)-(2x-4)\cdot(1,-3x)=(-2x+4,1+3x(2x-4))=(3x+4,x^2+3x+1)$ (nell'ultimo passaggio, oltre a effettuare i calcoli siamo passati a scrivere i rappresentanti canonici delle classi resto modulo 5).

Da ciò, moltiplicando tutto per $3=2^{-1}$, si ha $1=(4x+2)f+(3x^2+4x+3)g$, e quindi la coppia $(4x+2,\,3x^2+4x+3)$ è una coppia di coefficienti di Bezout per esprimere $1=MCD(f,g)$. □

Esercizio 41. *Sia $f=x^3-x+2\in\mathbb{Z}_3[x]$, e sia $R:=\mathbb{Z}_3[x]/(f)$ il relativo anello quoziente. Detti $\alpha:=[2x^2+x-1]_f, \beta:=[x^2+2x+1]_f$, determinare $\alpha+\beta$ e $\alpha\beta$.*

***Svolgimento Esercizio* 41.** Si ha

$$\begin{aligned}\alpha+\beta =&[2x^2+x-1]_f+[x^2+2x+1]_f=[(2x^2+x-1)+(x^2+2x+1)]_f\\ &=[3x^2+3x]_f=[0]_f\\ \alpha\cdot\beta=&[2x^2+x-1]_f\cdot[x^2+2x+1]_f=[(2x^2+x-1)(x^2+2x+1)]_f\\ &=[2x^4+2x^3-x-1]_f,\end{aligned}$$

ma il polinomio ottenuto non ha grado $<3=\partial f$. Dobbiamo perciò ridurlo modulo f: dato che $2x^4+2x^3-x-1=f\cdot(2x+2)+(2x^2+1)$, si ha $[2x^4+2x^3-x-1]_f=[2x^2+1]_f$. Questa classe (elemento di R) è il risultato del prodotto $\alpha\beta$. □

Esercizio 42. *Sia $f=2x^3-x^2+2x-1\in\mathbb{Z}_5[x]$ e sia R l'anello quoziente $\mathbb{Z}_5[x]/(f)$. Determinare se l'elemento $\alpha:=[2x^2-3x+1]_f$ è in $\mathscr{U}(R)$ oppure è un divisore dello zero in R. Nel primo caso, esibire il suo inverso, nel secondo un codivisore non banale di zero.*

***Svolgimento Esercizio* 42.** Il calcolo del MCD tra f e il polinomio $g:=2x^2-3x+1$ decide tutto: si ha $f=(x+1)g+(4x-2)$ e $g=(3x-3)(4x-2)$, per cui $m:=4x-2$ è un MCD tra f e g. Il $MCD(f,g)$ si ottiene normalizzando il polinomio m, cioè moltiplicando m per l'inverso del suo coefficiente direttore, $4^{-1}=4$, ottenendo $d=x+2=MCD(f,g)$. Poichè $MCD(f,g)\neq 1 \Rightarrow \alpha$ è un divisore dello zero in R.

Per avere un co-divisore di zero non banale, basta calcolare $f':=f/d$. Si ottiene $f=(2x^2+2)(x+2)$, per cui un co-divisore di zero per α è presto ottenuto: basta prendere $f':=2x^2+2$ e considerare la sua classe $\beta:=[f']_f$. Infatti si ha $\beta\neq 0$ (perchè $f'\neq 0$ e ha grado più basso di quello di f) e

$$\alpha\beta=[gf']_f=[g'df']_f=[g'f]_f=[0]_f=0_R,$$

dove come al solito $g':=g/d=2x+3$. □

Esercizio 43. *Sia $f:=x^2-1\in\mathbb{Z}_5[x]$ e si consideri l'anello quoziente $R:=\mathbb{Z}_5[x]/(f)$. Determinare se l'elemento $\alpha:=[2x+1]_f\in R$ è invertibile oppure è un divisore dello zero in R. Nel primo caso, esibire il suo inverso, nel secondo un codivisore non banale di zero.*

***Svolgimento Esercizio* 43.** Detto $g:=2x+1\in\mathbb{Z}_5[x]$, calcoliamo $MCD(f,g)$. Si ha $f=(2x+1)(3x+1)+3$, per cui $MCD(f,g)=1$ e quindi α è invertibile.

Per calcolare il suo inverso, dal fatto che $3 = f - (3x+1)g$ si ha anche che $1 = 2f - 2(3x+1)g$, cioè $\alpha^{-1} = [-2(3x+1)]_f = [4x+3]_f$, cioè la classe modulo f del coefficiente di Bezout di g nell'espressione di $1 = MCD(f,g)$. Come verifica, si ha

$$(2x-1)(4x+3) = 3x^2 + 3 = 3(x^2-1) + 1 \equiv 1 \pmod{x^2-1}.\square$$

Esercizio 44. *Sia $f := x^2+1 \in \mathbb{Z}_5[x]$, e sia $R := \mathbb{Z}_5[x]/(f)$. Decidere se R è un campo o non è un campo.*

***Svolgimento Esercizio* 44.** Sappiamo che R è un campo $\iff$ f è un polinomio irriducibile di $\mathbb{Z}_5[x]$. Dato che ha grado 2, basta controllare se ha o non ha radici in $\mathbb{Z}_5$. Si scopre subito che 2 è una radice di f: $2^2+1 = 5 = 0$. Perciò, f è un multiplo di $x-2$ (per il Teorema di Ruffini), e quindi non è irriducibile. Si può concludere che R NON è un campo.

Alla stessa conclusione si poteva arrivare anche per altra via: notato che $x^2 + 1 = x^2 - 4$ (i coefficienti sono in $\mathbb{Z}_5$!), sappiamo dall'algebra elementare che $f = (x-2)(x-3)$, e cioè che f ha non una, ma due radici in $\mathbb{Z}_5$, precisamente 2 e 3. Sappiamo perciò non solo che R NON è un campo, ma anche come è fatto: usando il TCR, si ha $R = \mathbb{Z}_5[x]((x-2)(x-3)) \cong \mathbb{Z}_5[x]/(x-2) \oplus \mathbb{Z}_5[x]/(x-3) \cong \mathbb{Z}_5 \oplus \mathbb{Z}_5$, una somma diretta di campi. $\square$

Esercizio 45. *Sia $f := x^2+1 \in \mathbb{Z}_3[x]$, e sia $R := \mathbb{Z}_3[x]/(f)$. Decidere se R è un campo o non è un campo.*

***Svolgimento Esercizio* 45.** Con lo stesso ragionamento di prima, scopriamo che il polinomio x^2+1 E' irriducibile in $\mathbb{Z}_3[x]$, perchè non ha radici in $\mathbb{Z}_3$ e ha grado 2. Infatti, $f(0) = 1$, $f(1) = 2 = f(2)$. Perciò, l'anello quoziente è un campo, con esattamente 9 elementi. A parte $[0]_f$, tutti gli altri 8 elementi sono invertibili.

Esercizio 46. *Sia $f(x) = x^3 + 1 \in \mathbb{Z}_3[x]$.*

1. *Si dica se l'anello quoziente $A := \mathbb{Z}_3[x]/(f)$ è o meno un campo, motivando la risposta;*
2. *si dica se l'elemento $[2x^2+1] \in A$ è invertibile o un divisore dello zero in A, motivando la risposta;*
3. *si esibisca l'inverso di $[2x^2+1]$ o un suo co-divisore di zero, a seconda della precedente risposta.*

***Svolgimento Esercizio* 46.** Il polinomio f è riducibile: questo segue tanto dall'algebra elementare, perchè $x^3+1 = (x+1)(x^2-x+1)$ è un noto prodotto notevole, quanto dal Teorema di Ruffini, perchè è evidente che $f(2) = 8+1 = 0 \in \mathbb{Z}_3$, e quindi f ha almeno la radice 2 in $\mathbb{Z}_3$. Di conseguenza, A NON è un campo.

Per vedere se $[2x^2+1]$ è invertibile o meno, basta calcolare il suo MCD con f: ciò si può calcolare tramite l'algoritmo euclideo, ma anche osservando che il polinomio $2x^2+1 \in \mathbb{Z}_3[x]$ si fattorizza in $2x^2+1 = 2(x^2+2) = 2(x^2-1) = 2(x+1)(x-1)$, e poichè $(x-1) \nmid f$ (altrimenti $f(1) = 0$, cosa che non è!) $\Rightarrow MCD(f, 2x^2+1) = x+1$, il polinomio irriducibile monico che è fattore comune a f e a $2x^2+1$. Pertanto, $[2x^2+1]$ è un divisore di zero in A.

Per avere, infine, un co-divisore di zero di $[2x^2+1]$, basta prendere la classe $[x^2-x+1] \in A$, che è non nulla (perchè il grado di x^2-x+1 è minore di quello di f) e $[2x^2+1][x^2-x+1] = (2[x-1][x+1])[x^2-x+1] = 2[x-1][(x+1)(x^2-x+1)] = 2[x-1][f] = 0_A$.

Per la cronaca, la fattorizzazione completa di $f = x^3+1$ è $f = (x+1)^3$, come si può controllare direttamente. $\square$

5. Matrici quadrate a coefficienti in un campo

Fissato $n \geqslant 1$, creiamo una tabella, delimitata da una coppia di parentesi e costituita da n^2 case, disposte secondo n righe ed n colonne. La casa all'incrocio tra la riga i e la colonna j la chiamiamo casa (i,j). Sia poi X un *insieme* qualunque.

Definizione 5.1. Diciamo matrice quadrata a entrate in X di ordine n ogni tabella $n \times n$ le cui case siano state riempite con elementi di X. L'insieme delle matrici così ottenute si indica con $M_n(X)$. L'elemento che occupa la casa (i,j) si dice l'entrata (i,j) o (i,j)-*entrata* della matrice. Due matrici sono *uguali* se hanno le stesse entrate, casa per casa.

Per esempio, sia $X = \{\partial, 1, \mathbb{Z}_2\}$, ed $n = 2$. La matrice $\begin{pmatrix} 1 & \partial \\ \partial & \mathbb{Z}_2 \end{pmatrix}$ è uno degli elementi di $M_2(X)$. L'entrata $(1,2)$ è il simbolo ∂, elemento di X, l'entrata $(2,2)$ è l'insieme $\mathbb{Z}_2$, elemento di X.

A noi interessano solo le matrici quadrate a entrate (*a coefficienti*) in un campo F: $M_n(F)$. Molte delle considerazioni però restano valide anche se prendiamo le entrate in un anello commutativo con unità (p.es.: $X = \mathbb{Z}$). Inoltre, nell'ultima sezione di queste note, considereremo anche matrici NON necessariamente quadrate, in cui il numero m di righe può essere diverso dal numero n di colonne. L'insieme di tali matrici verrà allora denotato con $M_{m\times n}(F)$; in pratica, la scrittura $M_n(F)$ è una scrittura semplificata per indicare $M_{n\times n}(F)$.

Osservazione 5.2. A parte i campi $\mathbb{Q}$ ed $\mathbb{R}$, conosciamo i campi $\mathbb{Z}_p$, dove p è un primo positivo. Il problema nel considerare matrici a coefficienti in $\mathbb{Z}_p$ è che si viene subito a creare un eccesso di parentesi e indici, dovendo scrivere per esempio $[a_{ij}]_p$ per indicare che l'entrata (i,j) della matrice considerata è la classe modulo p dell'intero a_{ij}. Al fine di semplificare la notazione, perciò, si scrive direttamente a_{ij} intendendo $[a_{ij}]_p \in \mathbb{Z}_p$. Così, dire che $\mathbf{a} = (a_{ij}) \in M_n(\mathbb{Z}_p)$ vuol dire che $\mathbf{a}$ è una matrice $n \times n$, in cui l'entrata (i,j) è l'elemento $[a_{ij}]_p \in \mathbb{Z}_p$. Con questo abuso, la notazione diventa meno formale ma più trattabile, e la utilizzeremo diffusamente.

Definizione 5.3. ***(Addizione tra matrici)***
Date $\mathbf{a}, \mathbf{b} \in M_n(F)$, la *somma* $\mathbf{a} + \mathbf{b}$ è la matrice di $M_n(F)$ avente come entrata (i,j) la somma delle entrate (i,j) di $\mathbf{a}$ e $\mathbf{b}$.

Esercizio 47. *Con questa addizione $(M_n(F), +)$ è un gruppo abeliano. Il suo elemento neutro è denotato $\mathbf{0}_n$, ed è la matrice $n \times n$ avente tutte le entrate nulle.*

Definizione 5.4. ***(Prodotto tra matrici)***
Se $\mathbf{a} = (a_{ij}), \mathbf{b} = (b_{ij}) \in M_n(F)$, il *prodotto* $\mathbf{a} \cdot \mathbf{b}$ è la matrice $\mathbf{c} = (c_{ij}) \in M_n(F)$ avente, per ogni i, j, entrata (i,j)

$$c_{ij} := a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj} = \sum_{k=1}^{n} a_{ik}b_{kj}$$

(prodotto *righe per colonne*).

***Esempio* 5.5.** Scrivendo

$$\mathbf{a} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \in M_3(\mathbb{Z}_3)$$

si intende che le entrate (i coefficienti) sono prese in $\mathbb{Z}_3$; quindi $0, 1, 2$ sono intesi come le classi $[0]_3, [1]_3, [2]_3$ rispettivamente, e i calcoli tra le entrate delle matrici sono computate in $\mathbb{Z}_3$. Si ha perciò

$$\mathbf{c} = \mathbf{a} \cdot \mathbf{b} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Infatti, l'entrata c_{11} del posto $(1,1)$ di $\mathbf{c}$ si calcola considerando la *riga 1 di* $\mathbf{a}$ e la *colonna 1 di* $\mathbf{b}$,

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \rightsquigarrow c_{11} = 1 \cdot 0 + 0 \cdot 0 + 2 \cdot 0 = 0,$$

l'entrata $(1,2)$ di $\mathbf{c}$ (c_{12}) si calcola considerando la *riga 1 di* $\mathbf{a}$ e la *colonna 2 di* $\mathbf{b}$

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \rightsquigarrow c_{12} = 1 \cdot 1 + 0 \cdot 1 + 2 \cdot 0 = 1,$$

l'entrata $(1,3)$ di $\mathbf{c}$ si calcola considerando la *riga 1 di* $\mathbf{a}$ e la *colonna 3 di* $\mathbf{b}$

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \rightsquigarrow c_{13} = 1 \cdot 2 + 0 \cdot 1 + 2 \cdot 2 = 2 + 1 = 0,$$

e così via per il calcolo delle altre entrate c_{ij} nelle rimanenti case (i,j) di $\mathbf{c}$.

Osservazione 5.6. Il prodotto righe per colonne funziona anche per matrici non quadrate, purchè il numero di colonne della prima matrice coincida con il numero di righe della seconda. In parole povere, se $\mathbf{a} \in M_{m\times n}(F)$ e $\mathbf{b} \in M_{n\times p}(F)$, il prodotto righe per colonne può essere effettuato per calcolare la matrice $\mathbf{ab} \in M_{m\times p}(F)$, mentre il prodotto $\mathbf{ba}$ NON può essere calcolato, a meno che $p = m$. Per il momento, comunque, lavoreremo solo con matrici quadrate. □

Esercizio 48. La matrice avente 1_F nelle case diagonali (i,i) e 0_F in tutte le altre è elemento neutro per il prodotto in $M_n(F)$, e la si denota con $\mathbf{1}_n$.

Proposizione 5.7. *La struttura $(M_n(F), +, \cdot)$ è un anello con unità, NON commutativo non appena $n \geqslant 2$. Il suo gruppo degli elementi invertibili si denota con $GL_n(F)$ e si dice il* gruppo lineare generale di ordine n su F.

***Esempio* 5.8.** Quale che sia F, si ha

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Ciò fornisce non solo la prova che l'anello non è commutativo, ma anche un esempio di anello in cui accade che $b \cdot a = 0_A$ ma $a \cdot b \neq 0_A$, giustificando la distinzione tra *divisore destro di zero* e *divisore sinistro di zero*.

E' vero, ma non ovvio, che $\mathbf{a} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ è anche un divisore sinistro di zero, e cioè esiste *anche* una matrice $\mathbf{c} \in M_2(\mathbb{Z}_3)$ tale che $\mathbf{a} \cdot \mathbf{c} = \mathbf{0}_2$, solo che $\mathbf{c} \neq \mathbf{b} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Per esempio, basta prendere $\mathbf{c} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Notare che $\mathbf{c} \cdot \mathbf{a} = \mathbf{c}$. □

Non è facile capire direttamente se una data matrice è o non è invertibile:

***Esempio* 5.9.** Quale che sia il campo F, la matrice $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(F)$ non è invertibile.
Invece la matrice $\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \in M_2(\mathbb{Z}_3)$ è invertibile: infatti

$$\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{1}_n.$$

Esercizio 49. *Siano A un anello (non commutativo) con unità e a un suo elemento. Se a è invertibile sia a destra che a sinistra $\Rightarrow a \in \mathscr{U}(A)$. Cioè: se esistono $u, v \in A$ tali che $ua = 1_A$ e $av = 1_A$ allora $u = v$ (e tale elemento si indica senza ambiguità con a^{-1}).*

Definizione 5.10. Data una matrice $\mathbf{a} = (a_{ij}) \in M_n(F)$, l'elemento

$$\det(\mathbf{a}) := \sum_{\sigma \in S_n} (-1)^\sigma a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)} \in F$$

si dice il *determinante* di $\mathbf{a}$.

***Esempio* 5.11.** Se $\mathbf{a} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(F)$, è $\det(\mathbf{a}) = \sum_{\sigma \in S_2} (-1)^\sigma a_{1\sigma(1)} a_{2\sigma(2)}$; dato che $S_2 = \{id, (1\,2)\}$, si ha

$$\det(\mathbf{a}) = \underset{\sigma = id}{\underset{\downarrow}{a_{11}a_{22}}} + \underset{\sigma = (1\,2)}{\underset{\downarrow}{(-1)^{(1\,2)} a_{12}a_{21}}} = a_{11}a_{22} - a_{12}a_{21}.$$

Il determinante di una matrice 3×3 si ottiene facendo variare σ in $S_3 = \{id, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$, e si ha

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{array}{l} a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ -(a_{13}a_{22}a_{31} + a_{12}a_{21}a_{33} + a_{11}a_{23}a_{32}). \end{array}$$

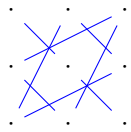
(*regola di Sarrus*). Se la taglia delle matrici è $\geqslant 4$ le formule diventano troppo complicate, perchè compaiono $n!$ addendi. In tal caso, i determinanti si calcolano usando il cosiddetto *sviluppo secondo una riga o secondo una colonna* (Formule di Laplace).

***Esempio* 5.12.** Data la matrice $\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \in M_2(\mathbb{Z}_3)$, è

$$\det \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} = 2 - 4 = 1 \in \mathbb{Z}_3.$$

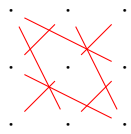
Esercizio 50. *Calcolare il determinante della matrice* $\mathbf{a} := \begin{pmatrix} 1 & 0 & 3 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix} \in M_3(\mathbb{Z}_5)$.

Svolgimento Poichè $n = 3$, dobbiamo usare la regola di Sarrus: calcoliamo prima i prodotti con segno $+$, cioè $a_{11}a_{22}a_{33}$, $a_{12}a_{23}a_{31}$, $a_{13}a_{21}a_{32}$, poi quelli con segno $-$, cioè $a_{13}a_{22}a_{31}$, $a_{12}a_{21}a_{33}$, $a_{11}a_{23}a_{32}$, prendendo cioè i prodotti tra le entrate della matrice scelti come segue



$1+0+2=3$

$$\Rightarrow \quad \det(\mathbf{a}) = 3 - 0 = 3$$



$0+0+0=0$

□

Tra le matrici, alcune di forma particolare sono molto utili:

Definizione 5.13. Data una matrice $\mathbf{a} \in M_n(F)$, la diagonale costituita dalle case $(1,1),(2,2),\dots,(n,n)$ si dice la diagonale principale della matrice.

Definizione 5.14. Una matrice si dice triangolare superiore se tutte le entrate sotto la diagonale principale sono nulle. Una matrice si dice diagonale se tutte le entrate al di fuori della diagonale principale sono nulle.

Analogamente si definiscono le matrici triangolari inferiori.

***Esempio* 5.15.** Le matrici $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ sono triangolari superiori. La matrice $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ è diagonale. La matrice $\mathbf{1}_n$ è diagonale. Così pure la matrice nulla $\mathbf{0}_n$. Ogni matrice diagonale è sia triangolare superiore sia triangolare inferiore.

Se le matrici hanno una di queste forme particolari, è facile calcolarne il determinante. Nel prossimo risultato elenchiamo i (pochi!) casi in cui il calcolo del determinante di una matrice (anche di ordine elevato) è immediato.

Proposizione 5.16.

- *Se una matrice ha una riga o una colonna nulla $\Rightarrow$ il suo determinante è zero. La stessa cosa accade se la matrice ha due righe uguali, o due colonne uguali;*
- *se una matrice è triangolare (in particolare: se è diagonale) $\Rightarrow$ il suo determinante è il prodotto degli elementi sulla diagonale.*

Teorema 5.17.

(1) *(Teorema di Binet) Il determinante preserva il prodotto tra matrici:*

$$\forall \mathbf{a}, \mathbf{b} \in M_n(F) \qquad \det(\mathbf{a} \cdot \mathbf{b}) = \det(\mathbf{a}) \cdot \det(\mathbf{b});$$

(2) $\mathbf{a} \in M_n(F)$ *è invertibile* $\iff \det(\mathbf{a}) \neq 0$*;*
(3) $\det(\mathbf{a}) = 0 \iff \mathbf{a}$ *è un divisore di zero in* $M_n(F)$*.*

Alla luce del precedente Teorema, il determinante gioca il ruolo che il MCD giocava per gli anelli $\mathbb{Z}_n$ e per gli anelli quoziente $F[x]/(f)$: se $\mathbf{a} \in M_n(F)$ è una matrice non nulla, basta calcolare $\det(\mathbf{a})$ per sapere se la matrice data è invertibile o un divisore di zero.

Corollario 5.18. *La funzione* $\det : GL_n(F) \to F^*$ *è suriettiva. Inoltre, l'anello delle matrici è ripartito in* $M_n(F) = \{\mathbf{0}_n\} \uplus \mathscr{D}(M_n(F)) \uplus \mathscr{U}(M_n(F))$.

Osservazione 5.19.

(1) det non preserva l'addizione: $\det(\mathbf{a}+\mathbf{b}) \neq \det(\mathbf{a}) + \det(\mathbf{b})$. Per esempio,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

ma $\det(\mathbf{1}_2) = 1_F$, mentre ciascuno degli addendi a secondo membro ha determinante 0_F.

(2) Il determinante ci dice solo se una matrice è invertibile o meno ma, se $\mathbf{a}$ è invertibile, non ci dice *chi* sia l'inversa. Tuttavia è possibile usare il determinante per calcolare la matrice inversa di una matrice invertibile. Non tratteremo questa questione (inversione tramite la *matrice aggiunta*) nel nostro corso.

***Esempio* 5.20.** Abbiamo visto che la matrice $\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \in M_2(\mathbb{Z}_3)$ ha determinante $1 \in \mathbb{Z}_3 \Rightarrow$ sappiamo che è invertibile, ma non abbiamo modo di sapere che l'inversa è la matrice $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$.

Solo nel caso di una matrice invertibile di ordine 2 è facile calcolare la sua inversa tramite il suo determinante. Vale infatti la seguente formula:

Esercizio 51. *Sia* $\mathbf{a} = \begin{pmatrix} u & v \\ w & z \end{pmatrix} \in M_2(F)$, *e sia* $d := \det(\mathbf{a})$. *Verificare che, se* $d \neq 0$, *allora*

$$\mathbf{a}^{-1} = d^{-1} \begin{pmatrix} z & -v \\ -w & u \end{pmatrix} := \begin{pmatrix} zd^{-1} & -vd^{-1} \\ -wd^{-1} & ud^{-1} \end{pmatrix}.$$

***Esempio* 5.21.** Per $\mathbf{a} = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \in M_2(\mathbb{Z}_3) \Rightarrow d = \det(\mathbf{a}) = 1 \Rightarrow \mathbf{a}^{-1} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, come affermato prima.

Attenzione! Come detto, questo vale SOLO per matrici 2×2! E' altamente sconsigliabile *tentare* di ricostruire l'inversa già di una matrice 3×3 con varianti più o meno fantasiose del metodo usato per matrici 2×2!

Operazioni elementari sulle righe

Sia $\mathbf{a} \in M_n(F)$. Ci sono tre tipi di operazioni sulle righe di $\mathbf{a}$ che servono a produrre altre matrici:

(1) dato $\alpha \in F^*$, $\boxed{R_{ij}(\alpha)}$ denota l'operazione che altera solo la riga i di $\mathbf{a}$, e precisamente *alla riga* i *di* $\mathbf{a}$ *aggiunge la riga* j *di* $\mathbf{a}$ *moltiplicata per* α;

(2) dato $\alpha \in F^*$, $\boxed{\mu_i(\alpha)}$ denota l'operazione che altera solo la riga i di $\mathbf{a}$, moltiplicando ogni suo elemento per α;

(3) $\boxed{T_{ij}}$ denota l'operazione che scambia tra loro le righe i e j di $\mathbf{a}$.

***Esempio* 5.22.** Lavorando in $M_3(\mathbb{Z}_3)$ si ha

$$\begin{pmatrix}1&0&2\\0&0&2\\1&2&0\end{pmatrix} \underset{R_{31}(2)}{\to} \begin{pmatrix}1&0&2\\0&0&2\\0&2&1\end{pmatrix} \underset{T_{23}}{\to} \begin{pmatrix}1&0&2\\0&2&1\\0&0&2\end{pmatrix} \underset{\mu_2(2)}{\to} \begin{pmatrix}1&0&2\\0&1&2\\0&0&2\end{pmatrix}$$

$$\underset{R_{13}(2)}{\to} \begin{pmatrix}1&0&0\\0&1&2\\0&0&2\end{pmatrix} \underset{R_{23}(2)}{\to} \begin{pmatrix}1&0&0\\0&1&0\\0&0&2\end{pmatrix} \underset{\mu_3(2)}{\to} \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} = \mathbf{1}_3$$

Teorema 5.23. (Inversione di una matrice)
Data una matrice $\mathbf{a} \in M_n(F)$*, essa è invertibile* $\iff$ *esiste una sequenza di trasformazioni elementari sulle righe al termine delle quali si ottiene la matrice* $\mathbf{1}_n$*. In tal caso la stessa sequenza, applicata alla matrice* $\mathbf{1}_n$*, fornisce la matrice inversa di* $\mathbf{a}$*.*

Nell'esempio più sopra, al termine della sequenza $R_{31}(2), T_{23}, \mu_2(2), R_{13}(2), R_{23}(2), \mu_3(2)$ avevamo ottenuto la matrice $\mathbf{1}_3 \Rightarrow$ la matrice di partenza è invertibile. La stessa sequenza, applicata alla matrice $\mathbf{1}_3$, ce ne dà l'inversa:

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \underset{R_{31}(2)}{\to} \begin{pmatrix}1&0&0\\0&1&0\\2&0&1\end{pmatrix} \underset{T_{23}}{\to} \begin{pmatrix}1&0&0\\2&0&1\\0&1&0\end{pmatrix} \underset{\mu_2(2)}{\to} \begin{pmatrix}1&0&0\\1&0&2\\0&1&0\end{pmatrix}$$

$$\underset{R_{13}(2)}{\to} \begin{pmatrix}1&2&0\\1&0&2\\0&1&0\end{pmatrix} \underset{R_{23}(2)}{\to} \begin{pmatrix}1&2&0\\1&2&2\\0&1&0\end{pmatrix} \underset{\mu_3(2)}{\to} \begin{pmatrix}1&2&0\\1&2&2\\0&2&0\end{pmatrix}$$

Osservazione 5.24.

(1) La sequenza NON è univocamente determinata, ma l'esito finale NON dipende dalla sequenza scelta.
(2) Se la matrice di partenza ha un'intera colonna nulla, è certamente non invertibile. Se la matrice non ha colonne nulle ma a un certo punto, durante le trasformazioni, si ottiene una matrice in cui un'intera riga è nulla $\Rightarrow$ è inutile continuare: la matrice non è invertibile.
(3) E' importante l'ordine con cui si susseguono le trasformazioni elementari: effettuare prima $R_{12}(u)$ e poi $\mu_1(\alpha)$ produce una matrice, effettuare prima $\mu_1(\alpha)$ e poi $R_{12}(u)$ ne produce un'altra! Solo in certe circostanze può capitare che l'esito di due trasformazioni elementari consecutive non dipenda dall'ordine con cui le si eseguono.
(4) E' possibile dare un algoritmo esplicito (da implementare) che accetta in input una matrice e dà in output la sequenza delle trasformazioni per la sua inversione o la certificazione che la matrice è un divisore dello zero. Non è questa la sede per illustrarla: per i nostri scopi, basta un po' di logica e di esperienza per scoprire quali trasformazioni concrete servano per una data matrice.

Esercizio 52. *Determinare per quali valori di* $c \in \mathbb{Z}_7$ *la seguente matrice di* $M_4(\mathbb{Z}_7)$ *è invertibile:*

$$\begin{pmatrix}1&2&3&4\\2&3&4&5\\3&4&c&6\\4&5&6&c^2\end{pmatrix}$$

Svolgimento Esercizio 52. Possiamo usare le trasformazioni elementari per rispondere alla domanda. Notare che la stessa chiede informazioni sull'*invertibilità*, e non la *determinazione dell'inversa!* Si ha:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & c & 6 \\ 4 & 5 & 6 & c^2 \end{pmatrix} \underset{\substack{R_{21}(5)\\ R_{31}(4)\\ R_{41}(3)}}{\rightarrow} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 6 & 5 & 4 \\ 0 & 5 & 5+c & 1 \\ 0 & 4 & 1 & 5+c^2 \end{pmatrix} \underset{\mu_2(6)}{\rightarrow}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 5 & 5+c & 1 \\ 0 & 4 & 1 & 5+c^2 \end{pmatrix} \underset{\substack{R_{32}(2)\\ R_{42}(3)}}{\rightarrow} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 2+c & 0 \\ 0 & 0 & 0 & c^2 \end{pmatrix}$$

per cui la matrice è invertibile $\iff c \neq 0, 5$ (ovvero $c \in \{1, 2, 3, 4, 6\}$): se $c = 0$ è nulla tutta la quarta riga, se invece $c = 5$ allora nella casa diagonale $(3, 3)$ compare 0, e non è più possibile ottenere la matrice $\mathbf{1}_4$ (perchè il determinante della matrice ottenuta è 0, e quindi non è invertibile: da lì in poi non ci sono speranze di ottenere $\mathbf{1}_4$ tramite successive trasformazioni elementari sulle righe!). □

E' possibile usare le trasformazioni elementari anche per semplificare il calcolo dei determinanti: nel seguito, siano t una trasformazione elementare, $\mathbf{a}$ una matrice, e $\mathbf{b}$ la matrice ottenuta applicando ad $\mathbf{a}$ la trasformazione t, cioè $\mathbf{a} \underset{t}{\rightarrow} \mathbf{b}$. Allora

- se $t = R_{ij}(\alpha) \Rightarrow \det(\mathbf{b}) = \det(\mathbf{a})$;
- se $t = \mu_i(\alpha) \Rightarrow \det(\mathbf{b}) = \alpha \det(\mathbf{a})$;
- se $t = T_{ij} \Rightarrow \det(\mathbf{b}) = -\det(\mathbf{a})$.

Tenendo traccia di queste regole, possiamo usare le trasformazioni elementari e portare $\mathbf{a}$ ad una matrice triangolare $\mathbf{b}$. Fatto ciò, si può calcolare il determinante di $\mathbf{b}$ e conoscere il determinante di $\mathbf{a}$.

Esercizio 53.

Calcolare il determinante della matrice $\mathbf{a} = \begin{pmatrix} 1 & 0 & 2 & 4 \\ 2 & 0 & 3 & 2 \\ 0 & 2 & 2 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix} \in M_4(\mathbb{Z}_5)$.

Svolgimento Esercizio 53.

$$\begin{pmatrix} 1 & 0 & 2 & 4 \\ 2 & 0 & 3 & 2 \\ 0 & 2 & 2 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix} \underset{\substack{R_{21}(3)\\ R_{41}(2)}}{\rightarrow} \begin{pmatrix} 1 & 0 & 2 & 4 \\ 0 & 0 & 4 & 4 \\ 0 & 2 & 2 & 3 \\ 0 & 1 & 4 & 0 \end{pmatrix} \underset{T_{24}}{\rightarrow} \begin{pmatrix} 1 & 0 & 2 & 4 \\ 0 & 1 & 4 & 0 \\ 0 & 2 & 2 & 3 \\ 0 & 0 & 4 & 4 \end{pmatrix} \underset{R_{32}(3)}{\rightarrow}$$

$$\begin{pmatrix} 1 & 0 & 2 & 4 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 4 & 3 \\ 0 & 0 & 4 & 4 \end{pmatrix} \underset{\mu_3(4)}{\rightarrow} \begin{pmatrix} 1 & 0 & 2 & 4 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 4 & 4 \end{pmatrix} \underset{R_{43}(1)}{\rightarrow} \begin{pmatrix} 1 & 0 & 2 & 4 \\ 0 & 1 & 4 & 0 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} =: \mathbf{b}$$

$$\Rightarrow 1 = \det(\mathbf{b}) = (-1) \cdot 4 \cdot \det(\mathbf{a}) = \det(\mathbf{a}).$$

Perciò, in questo caso, $\det(\mathbf{a}) = \det(\mathbf{b}) = 1$. □

Esercizio 54. *Sia* $\mathbf{a} = \begin{pmatrix} 2 & 0 \\ 1 & 4 \end{pmatrix} \in M_2(\mathbb{Z}_7)$.

(1) *Verificare che* $\mathbf{a} \in GL_2(\mathbb{Z}_7)$ *e determinarne l'inverso.*
(2) *Detto* $H := \langle \mathbf{a} \rangle \leqslant GL_2(\mathbb{Z}_7)$, *determinare* $|H|$*;*
(3) *trovare tutti gli altri elementi* $\mathbf{b} \in H$, $\mathbf{b} \neq \mathbf{a}$, *tali che* $\langle \mathbf{b} \rangle = H$.

***Svolgimento Esercizio* 54.** Si ha $\det(\mathbf{a}) = 1$, per cui $\mathbf{a}$ è invertibile, cioè un elemento di $GL_2(\mathbb{Z}_7)$. Per determinare l'inversa è inutile scomodare le trasformazioni elementari: possiamo usare la formula per invertire una matrice 2×2, ottenendo

$$\mathbf{a}^{-1} = \begin{pmatrix} 4 & 0 \\ 6 & 2 \end{pmatrix}.$$

Calcolare $|H|$ vuol dire calcolare il periodo (moltiplicativo) dell'elemento invertibile $\mathbf{a}$. Qui non abbiamo indizi sulla taglia di $|GL_2(\mathbb{Z}_7)|$, per cui dobbiamo effettivamente cercare il minimo intero positivo m tale che $\mathbf{a}^m = \mathbf{1}_2$. Si ha

$$\mathbf{a}^2 = \begin{pmatrix} 4 & 0 \\ 6 & 2 \end{pmatrix} = \mathbf{a}^{-1},$$

per cui siamo stati fortunati e possiamo concludere che $m = 3$. Dato che H è ciclico di ordine 3, c'è esattamente un altro generatore ciclico di H, precisamente $\mathbf{a}^2$ (che poi è appunto l'inversa di $\mathbf{a}$). □

Esercizio 55. *Sia* $R := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_3 \right\}$. *Si provi che* R *è un anello commutativo rispetto le usuali operazioni tra matrici. Quanti elementi ha* $\mathscr{U}(R)$*?*

***Svolgimento Esercizio* 55.** Bisogna prima provare che $(R, +)$ è un gruppo, e visto che R è contenuto in $M_2(\mathbb{Z}_3)$ facciamo prima a far vedere che è un sottogruppo del gruppo additivo di $M_2(\mathbb{Z}_3)$: basta provare che presa una coppia di elementi arbitrari in R, la loro differenza è ancora in R (si veda la Proposizione 8.1 a pag. 191 del libro di testo). In effetti, si ha

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} - \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} a - a' & b - b' \\ -(b - b') & a - a' \end{pmatrix} \in R.$$

Perciò, $R \leqslant (M_2(\mathbb{Z}_3), +)$. Poi bisogna verificare che R è chiuso per il prodotto, e cioè che presa una coppia di elementi qualunque in R il loro prodotto è ancora in R. In effetti si ha

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa' - bb' & ab' + a'b \\ -(ab' + a'b) & aa' - bb' \end{pmatrix} \in R.$$

Fatto ciò, è chiaro che $\cdot$ resta associativo e distributivo rispetto la somma (perchè lo è per tutte le matrici di $M_2(\mathbb{Z}_3)$, in particolare per quelle di R). Inoltre, $\mathbf{1}_2 \in R$ (si ottiene per $a = 1$ e $b = 0$). Perciò, $(R, +, \cdot)$ è un anello, e resta da verificare la proprietà commutativa del prodotto. Si ha infatti

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa' - bb' & ab' + a'b \\ -(ab' + a'b) & aa' - bb' \end{pmatrix} = \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} \cdot \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Con ciò, abbiamo provato che R è un anello commutativo.

Dobbiamo determinare $|\mathscr{U}(R)|$. Un elemento $\mathbf{u} \in R$ è invertibile in R se e solo se esiste un $\mathbf{v} \in R$ tale che $\mathbf{uv} = \mathbf{1}_2 = \mathbf{vu}$. Ciò ci dice che, in particolare, $\mathbf{u} \in GL_2(\mathbb{Z}_3)$ e quindi $\det(\mathbf{u}) \neq 0$. In altri termini, abbiamo appena provato che $\mathbf{u} \in \mathscr{U}(R) \Rightarrow \det(\mathbf{u}) \neq 0$, cosa peraltro abbastanza naturale.

Ciò che invece dobbiamo davvero provare è il converso di tale affermazione, e cioè che se $\mathbf{u} \in R$ e $\det(\mathbf{u}) \neq 0 \Rightarrow \mathbf{u} \in \mathscr{U}(R)$: a rigore, infatti, potrebbe accadere che l'elemento $\mathbf{u}^{-1}$ (che esiste sicuramente) NON sia in R, cioè che $\mathbf{u}$ pur essendo invertibile nell'anello "grande" $M_2(\mathbb{Z}_3)$ non sia invertibile in R.[5] Allora, sia $\mathbf{u} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, e $\det(\mathbf{u}) \neq 0$.

Sappiamo $\mathbf{u}^{-1} = (\det(\mathbf{u}))^{-1} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, che è un elemento di R.

Perciò, gli elementi invertibili di R sono precisamente quelli caratterizzati dal fatto di avere determinante non nullo. Poichè

$$\det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a^2 + b^2 = 0 \in \mathbb{Z}_3 \iff a = b = 0,$$

si ha che dei 9 elementi di R solo uno non è invertibile, per cui $|\mathscr{U}(R)| = 8$. Si noti che questo vuol dire che, forse un po' a sorpresa, R è addirittura un campo, finito e con 9 (numero non primo) elementi! □

Esercizio 56. *Sia* $\mathbf{a} = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \in M_3(\mathbb{Z}_5)$. *Provare che* $\mathbf{a}$ *è invertibile, e determinare inversa e periodo moltiplicativo di* $\mathbf{a}$.

***Svolgimento Esercizio* 56.** Il procedimento più diretto qui è usare subito le trasformazioni elementari: sapremo in un sol colpo se la matrice è invertibile e qual è la sua inversa. Si ha

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \underset{R_{12}(3)}{\to} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \underset{R_{31}(4)}{\to} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \mathbf{1}_3,$$

per cui non solo la matrice è invertibile, ma applicando la stessa sequenza di trasformazioni partendo dalla matrice $\mathbf{1}_3$ otteniamo

$$\mathbf{a}^{-1} = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \\ 4 & 2 & 1 \end{pmatrix}.$$

Incidentalmente, si noti che sappiamo anche che $\det(\mathbf{a}) = 1$ (anche se l'esercizio non ci chiede di calcolarlo).

Resta da calcolare il periodo moltiplicativo di $\mathbf{a}$. Si ha

$$\mathbf{a}^2 = \begin{pmatrix} 1 & 4 & 0 \\ 0 & 1 & 0 \\ 2 & 2 & 1 \end{pmatrix}, \ \mathbf{a}^3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 3 & 1 & 1 \end{pmatrix}, \ \mathbf{a}^4 = \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \\ 4 & 2 & 1 \end{pmatrix} = \mathbf{a}^{-1},$$

per cui il periodo cercato è 5. □

Un controesempio in Teoria dei Gruppi

In un gruppo $(G, \cdot)$ sappiamo che se $a, b \in G$ sono periodici e commutano allora ab è periodico, e il suo periodo divide $mcm(o(a), o(b))$.

Se però a, b NON commutano, questo è falso, e ab *potrebbe essere perfino non periodico*. Chiaro che per trovare un esempio ci serve un gruppo non commutativo

[5] Sarebbe tutt'altro che inusuale: considerando l'anello $\mathbb{Z}$, contenuto nell'anello $\mathbb{Q}$, l'elemento $2 \in \mathbb{Z}$ è invertibile in $\mathbb{Q}$, ma non lo è in $\mathbb{Z}$!

e infinito (altrimenti ogni elemento è periodico), e quindi non potevamo esibirne uno lavorando con i gruppi che abbiamo incontrato sinora (l'unico gruppo non abeliano incontrato prima è stato S_n, con $n \geqslant 3$, che però è finito). Ora abbiamo a disposizione il gruppo moltiplicativo $GL_2(\mathbb{Q})$, che è infinito e non abeliano, e possiamo cercare lì un esempio.

Esercizio 57. *Verificare che le seguenti matrici*

$$\mathbf{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ \mathbf{b} = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \ \mathbf{c} = \mathbf{a} \cdot \mathbf{b}$$

sono in $GL_2(\mathbb{Q})$. Determinare quali di esse sono periodiche e determinarne il periodo.

***Svolgimento Esercizio* 57.** Poichè $\det(\mathbf{a}) = 1 = \det(\mathbf{b}) \Rightarrow \mathbf{a}, \mathbf{b}$ sono invertibili $\Rightarrow \mathbf{c}$ è invertibile. Poi: $\mathbf{a}^2 = -\mathbf{1}_2 \Rightarrow o(\mathbf{a}) = 4$. Invece $\mathbf{b}^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ e $\mathbf{b}^3 = \mathbf{1}_2$ $\Rightarrow o(\mathbf{b}) = 3$.

Per $\mathbf{c}$, si ha

$$\mathbf{c} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \mathbf{c}^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \ \mathbf{c}^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \dots$$

e si può provare per induzione che per ogni $n \in \mathbb{N}$ si ha

$$\mathbf{c}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

per cui $\mathbf{c}$ NON è periodico. □

6. Applicazione: risoluzione di sistemi lineari

Assegnato un sistema lineare di m equazioni in n incognite a coefficienti in F, tutte le informazioni inerenti il problema sono codificate da una matrice con m righe (una per ciascuna equazione) ed $n+1$ colonne (una per ciascuna incognita, e una aggiuntiva per i termini noti). La matrice così ottenuta è detta *matrice completa del sistema*, e può essere suddivisa nella *matrice dei coefficienti* e nella *colonna dei termini noti*, con ovvio significato dei termini.

***Esempio* 6.1.** Le informazioni del sistema lineare a coefficienti in $\mathbb{Z}_{11}$

$$\begin{cases} 3x_1 + 2x_3 = 0 \\ 7x_1 + 2x_2 = 1 \\ x_1 + x_2 + 3x_3 = 2 \\ 2x_1 + x_2 + 3x_3 = 3 \\ x_2 + 2x_3 = 4 \end{cases}$$

sono tutte racchiuse nella sua matrice completa

$$\mathbf{s} := \left(\begin{array}{ccc|c} 3 & 0 & 2 & 0 \\ 7 & 2 & 0 & 1 \\ 1 & 1 & 3 & 2 \\ 2 & 1 & 3 & 3 \\ 0 & 1 & 2 & 4 \end{array}\right) \in M_{5\times 4}(\mathbb{Z}_{11}).$$

La riga verticale segna la separazione tra la matrice $\mathbf{a}$ dei coefficienti, e la colonna $\mathbf{c}$ dei termini noti. Esplicitamente,

$$\mathbf{a} = \begin{pmatrix} 3 & 0 & 2 \\ 7 & 2 & 0 \\ 1 & 1 & 3 \\ 2 & 1 & 3 \\ 0 & 1 & 2 \end{pmatrix}, \qquad \mathbf{c} = \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}.$$

Infatti, detta $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$, il sistema può essere riscritto in forma compatta come un'equazione lineare in $\mathbf{x}$: $\mathbf{ax} = \mathbf{c}$. Come si può controllare direttamente, sviluppando il prodotto matriciale $\mathbf{ax}$ si ottiene una matrice colonna le cui entrate sono esattamente il primo termine delle equazioni assegnate nel sistema. Nel seguito, scriveremo sinteticamente $\mathbf{s} = (\mathbf{a}|\mathbf{c})$ per indicare la matrice completa decomposta nella sua matrice dei coefficienti e la colonna dei termini noti. □

Quindi a ogni assegnato sistema lineare corrisponde una matrice a coefficienti in F (in genere, non quadrata), e chiaramente vale anche il viceversa: ogni matrice (anche non quadrata) può essere vista come la matrice completa di un sistema lineare.

Un sistema è risolubile se esiste almeno una n-pla di elementi di F, $(\alpha_1, \dots, \alpha_n) \in F^n$, tale che assegnando simultaneamente $x_i \leftarrow \alpha_i$ per ogni $i = 1, \dots, n$, tutte le risultanti uguaglianze del sistema sono soddisfatte. Se accade il contrario, il sistema si dice *non risolubile*, o *non compatibile*. La ragione dell'espressione *non compatibile* risiede nel fatto che ogni singola equazione può essere vista come un "vincolo" da soddisfare, per cui può ben accadere che ci sia un vincolo incompatibile con gli altri, e ciò rende il sistema non risolubile. Per esempio, il sistema

$$\begin{cases} 2x + y = 0 \\ 2x + y = 1 \end{cases}$$

è un sistema di due equazioni in due incognite che risulta incompatibile: la prima e la seconda equazione sono in contraddizione tra loro ($2x + y$ non può essere contemporaneamente 0 e 1). Come si capisce, più equazioni si aggiungono, più si rischia che il sistema non sia risolubile, e in questo il numero delle incognite c'entra poco: anche un sistema con una sola incognita può risultare incompatibile!

Per sistemi di piccola taglia (poche equazioni e poche incognite), c'è una certa varietà di tecniche risolutive (per sostituzione, per eliminazione, di Cramer, etc) incontrate nel percorso di scuola secondaria, e che risultano abbastanza efficaci. Queste tecniche elementari sono però ineffettive per sistemi con più di due/tre equazioni: risolvere un sistema con 5 equazioni è un compito abbastanza arduo, se affrontato con questi strumenti di base.

Per affrontare il problema in modo più efficace, possiamo usare le trasformazioni elementari. Il metodo che nasce si dice *di Gauss–Jordan*, e l'osservazione base è la seguente

Lemma 6.2. *Sia* $\mathbf{s} = (\mathbf{a}|\mathbf{c})$ *la matrice completa di un sistema lineare, e sia* $\mathbf{s}' = (\mathbf{a}'|\mathbf{c}')$ *la matrice ottenuta dopo aver effettuato una sequenza di trasformazioni elementari sulla matrice* $\mathbf{s}$. *Allora il sistema lineare di matrice completa* $\mathbf{s}'$ *è equivalente a quello di partenza.*

Dimostrazione. Basta controllare cosa acccade effettuando una singola trasformazione sulle righe: applicando una trasformazione $R_{ij}(\alpha)$ l'effetto sul sistema è quello di sommare membro a membro all'equazione i-ma l'equazione j-ma moltiplicata per α, applicando T_{ij} l'effetto è quello di scambiare di posto le equazioni i-ma e j-ma, e applicare $\mu_i(\alpha)$ vuol dire moltiplicare l'i-ma equazione per il numero $\alpha \neq 0$.

In tutti e tre i casi, il sistema risultante è perciò equivalente a quello di partenza. □

Possiamo usare quest'idea per portare il sistema di partenza nella forma più comoda possibile, la cui matrice completa sarà una matrice *in forma normale*:

Definizione 6.3. Una matrice $\mathbf{n}$ si dice *in forma normale* se:

(1) le righe non nulle di $\mathbf{n}$ sono tutte in alto, e consecutive;
(2) la prima entrata non nulla di ciascuna riga non nulla è 1; esso è detto il *pivot* della riga;
(3) scendendo lungo le righe, i pivot *scorrono lungo la destra*: il pivot della riga 2 è in una colonna a destra del pivot della riga 1, quello della riga 3 in una colonna a destra del pivot della riga 2, etc.
(4) nella colonna di ciascun pivot, il pivot è l'unica entrata non nulla: sopra e sotto di lui, in quella colonna, ci sono solo zeri;
(5) tutte le righe sotto l'ultimo pivot sono nulle.

***Esempio* 6.4.** La matrice

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

è in forma normale (qualunque sia il campo F); i tre pivot (in rosso) sono nelle case $(1,2)$, $(2,4)$ e $(3,5)$.

Proposizione 6.5. *Se* $\mathbf{s}$ *è una qualunque matrice, esiste ed è unica una matrice in forma normale* $\mathbf{n}$*, ottenibile da* $\mathbf{s}$ *tramite una sequenza finita di trasformazioni elementari sulle righe. Tale matrice* $\mathbf{n}$ *si dice la forma normale di* $\mathbf{s}$.

Osservazione 6.6. Per determinare l'invertibilità e, nel caso, l'inversa, di una matrice quadrata, quel che facevamo era precisamente determinare la forma normale della matrice: se la matrice è quadrata ed è invertibile, la sua forma normale è invariabilmente la matrice identità (e viceversa)! Perciò, le stesse tecniche usate per le matrici quadrate ci portano verso la determinazione della forma normale di una generica matrice (anche non quadrata). □

***Esempio* 6.7.** Riprendendo la matrice $\mathbf{s}$ dell'esempio 6.1, ci sono varie sequenze di trasformazioni elementari possibili, che portano tutte verso la forma normale di $\mathbf{s}$, che nel caso in questione è

$$\mathbf{n} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

In altri termini: la matrice $\mathbf{n}$ è l'unica matrice in forma normale raggiungibile tramite una sequenza di trasformazioni elementari su $\mathbf{s}$. □

Determinata la forma normale della matrice completa, è facile decidere se il sistema è risolubile e, nel caso lo sia, quali sono le sue soluzioni: basta considerare il sistema di matrice completa $\mathbf{n} = (\mathbf{a}'|\mathbf{c}')$. Infatti, se uno dei pivot cade nella colonna $\mathbf{c}'$ dei termini noti, la corrispondente equazione sarà $0 = 1$, che chiaramente non ammette soluzioni, e il sistema risulta incompatibile.

Se invece tutti i pivot sono pivot anche per la matrice incompleta $\mathbf{a}'$ (cioè cadono tutti in $\mathbf{a}'$), allora il sistema è risolubile. Le incognite relative ai pivot hanno valore determinato dai valori assegnati alle incognite non relative ai pivot, e quale che siano i valori assegnati a queste incognite "libere", essi determinano un valore per le incognite pivotali.

***Esempio* 6.8.** Il sistema dell'esempio 6.1 non è risolubile, perchè uno dei pivot cade nella colonna dei termini noti.

Esercizio 58. *Si dica se il seguente sistema lineare a coefficienti in* $\mathbb{Z}_7$

$$\begin{cases} x_1 & +2x_2 & +3x_3 & = 4 \\ 2x_1 & & +3x_3 & = 5 \\ 3x_1 & +2x_2 & & = 6 \end{cases}$$

è compatibile e, se sì, si dica quante e quali sono le sue soluzioni

***Svolgimento Esercizio* 58.** La matrice dei coefficienti, la colonna dei termini noti e la matrice completa sono rispettivamente

$$\mathbf{a} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 0 & 3 \\ 3 & 2 & 0 \end{pmatrix}, \qquad \mathbf{c} = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}, \qquad \mathbf{s} = \left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 2 & 0 & 3 & 5 \\ 3 & 2 & 0 & 6 \end{array}\right)$$

Tramite una sequenza di trasformazioni elementari, arriviamo alla forma normale della matrice completa $\mathbf{s}$:

$$\mathbf{n} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 4 \end{array}\right),$$

corrispondente al sistema lineare

$$\begin{cases} x_1 & = 0 \\ x_2 & = 3 \\ x_3 & = 4 \end{cases}$$

che ha come unica soluzione $(0, 3, 4) \in \mathbb{Z}_7^3$.

Esercizio 59. *Si dica se il seguente sistema lineare a coefficienti in* $\mathbb{Z}_7$

$$\begin{cases} 5x_1 & +2x_2 & +2x_3 & = 2 \\ 3x_1 & +4x_2 & +4x_3 & = 4 \\ 6x_1 & +6x_2 & +2x_3 & = 5 \end{cases}$$

è compatibile e, se sì, si dica quante e quali sono le sue soluzioni.

***Svolgimento Esercizio* 59.** La matrice dei coefficienti, la colonna dei termini noti e la matrice completa sono rispettivamente

$$\mathbf{a} = \begin{pmatrix} 5 & 2 & 2 \\ 3 & 4 & 4 \\ 6 & 6 & 2 \end{pmatrix}, \qquad \mathbf{c} = \begin{pmatrix} 2 \\ 4 \\ 5 \end{pmatrix}, \qquad \mathbf{s} = \left(\begin{array}{ccc|c} 5 & 2 & 2 & 2 \\ 3 & 4 & 4 & 4 \\ 6 & 6 & 2 & 5 \end{array}\right)$$

Tramite una sequenza di trasformazioni elementari, arriviamo alla forma normale della matrice completa $\mathbf{s}$:

$$\mathbf{n} = \left(\begin{array}{ccc|c} 1 & 0 & 2 & 4 \\ 0 & 1 & 3 & 5 \\ 0 & 0 & 0 & 0 \end{array}\right),$$

corrispondente al sistema lineare

$$\begin{cases} x_1 & & +2x_3 & = 4 \\ & x_2 & +3x_3 & = 5 \end{cases}$$

in cui x_3 può variare liberamente in tutto $\mathbb{Z}_7$. Ognuna delle 7 possibili assegnazioni di x_3 dà luogo a una assegnazione forzata di x_1 e x_2:

$$\text{posto } x_3 = y \in \mathbb{Z}_7 \text{ allora dev'essere } \begin{cases} x_1 = 4 - 2y \\ x_2 = 5 - 3y \end{cases}.$$

L'insieme delle soluzioni è allora

$$\{(4+5y, 5+4y, y) \mid y \in \mathbb{Z}_7\} = \{(4,5,0), (2,2,1), (0,6,2), (5,3,3), (3,0,4), (1,4,5), (6,1,6)\}.$$

Pertanto, ci sono 7^1 soluzioni distinte del sistema. □

Se un sistema è risolubile, non c'è bisogno di elencare le sue soluzioni per dire quante ce ne sono: bisogna passare per il seguente concetto

Definizione 6.9. Si dice rango di una matrice il numero dei pivot della sua forma normale.

Osservazione 6.10. Si noti che se la matrice è $m \times n$ allora il rango della matrice è $\leqslant \min\{m, n\}$: infatti su ciascuna riga e ciascuna colonna ci può essere al più un pivot. Nel caso di matrici quadrate, elementi di $M_n(F)$, dire che una matrice ha rango n equivale a dire che la matrice è invertibile (perchè la sua forma normale è $\mathbf{1}_n$). □

La risolubilità di un sistema lineare, e il numero delle sue soluzioni, è caratterizzato in termini classici dal seguente

Teorema 6.11. ***(Teorema di Rouchè-Capelli)***
Un sistema lineare è risolubile se e solo se il rango della matrice completa del sistema uguaglia quello della matrice dei coefficienti. In tal caso, se n è il numero delle incognite e ν è il rango, il sistema ha esattamente $|F|^{n-\nu}$ soluzioni distinte.

Dimostrazione. Detta al solito $\mathbf{s} = (\mathbf{a}|\mathbf{c})$ la matrice completa del sistema, dire che il rango di $\mathbf{s}$ uguaglia quello di $\mathbf{a}$ vuol dire precisamente che scritta la forma normale $\mathbf{n} = (\mathbf{a}'|\mathbf{c}')$ di $\mathbf{s}$, tutti i pivot di $\mathbf{n}$ cadono in $\mathbf{a}'$, e quindi il sistema è risolubile.

Inoltre, se ν è il rango di $\mathbf{a}$ e sono coinvolte n incognite, le ν incognite pivotali sono vincolate ai valori assunti dalle incognite libere, che sono in numero $n-\nu$. Per ciascuna incognita libera ci sono $|F|$ possibili assegnazioni, e ciascuna assegnazione alle incognite libere dà luogo a una distinta soluzione del sistema. Poichè ciascuna delle $n - \nu$ incognite libere può assumere $|F|$ valori distinti, per il principio di moltiplicazione si hanno esattamente $|F|^{n-\nu}$ soluzioni distinte del sistema. □

Osservazione 6.12. Ovviamente, se $|F| = \infty$ (come per esempio se $F = \mathbb{R}$ o $F = \mathbb{Q}$), un sistema lineare o non ha soluzioni, o ne ha esattamente una (precisamente quando $\nu = n$), oppure ne ha infinite (precisamente se $n > \nu$): $|F|^{n-\nu}$ non è più un

numero. Nella pratica, si continua a scrivere che *"il sistema ha $\infty^{n-\nu}$ soluzioni"*, con abuso di linguaggio, per dire che ci sono infinite soluzioni, ma dipendenti da $n-\nu$ parametri liberi. □

7. Esercizi sulle matrici

Esercizio 60. *Date le matrici*

$$\mathbf{a} = \begin{pmatrix} 1 & 2 \\ -1 & 2 \end{pmatrix}, \mathbf{b} = \begin{pmatrix} -1 & 2 \\ 1 & 1 \end{pmatrix}, \mathbf{c} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in M_2(\mathbb{Z}),$$

calcolare il valore delle seguenti espressioni:

(1) $\mathbf{a} + 2\mathbf{b} + 3\mathbf{c}$;
(2) $\mathbf{ab}$
(3) $\mathbf{c}^2$
(4) $\mathbf{b}^2 - 4\mathbf{ac}$;
(5) $(\mathbf{a} - \mathbf{b})^2$
(6) $\mathbf{a}^2 - 2\mathbf{ab} + \mathbf{b}^2$;
(7) $\mathbf{a}^2 - \mathbf{ab} - \mathbf{ba} + \mathbf{b}^2$.

Esercizio 61. *Si calcoli il prodotto* $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$.

Esercizio 62. *Si calcoli* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n$.

Esercizio 63. *Si trovi una formula per esprimere la potenza*

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^n$$

e la si provi per induzione.

Esercizio 64. *Siano* $\mathbf{a}, \mathbf{b}$ *matrici quadrate.*

(1) *Quando è vero che* $(\mathbf{a} + \mathbf{b})(\mathbf{a} - \mathbf{b}) = \mathbf{a}^2 - \mathbf{b}^2$*?*
(2) *Espandere la potenza* $(\mathbf{a} + \mathbf{b})^3$.

Esercizio 65. *Per ciascuno dei casi, determinare le matrici quadrate a coefficienti in* $\mathbb{Q}$ *che commutano con la matrice data*

(1) $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$
(2) $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$
(3) $\begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}$
(4) $\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$
(5) $\begin{pmatrix} 2 & 3 \\ 0 & 6 \end{pmatrix}$

Esercizio 66. *Calcolare, se possibile, le inverse delle seguenti matrici a coefficienti in* $\mathbb{R}$*:*

(1) $\begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 9 \\ 0 & -1 \end{pmatrix}$;

(2) $\begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 2 & 3 \\ 4 & -1 & 4 \\ 1 & 0 & 1 \end{pmatrix}$.

Quali di esse sono invertibili anche viste come matrici su $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$? In tali casi si determinino le loro inverse.

Esercizio 67. *Date le matrici $\mathbf{a}, \mathbf{b}$ a coefficienti in $F = \mathbb{Z}_3$, calcolare*

$$\mathbf{ab},\ \mathbf{a}+\mathbf{b},\ \mathbf{a}-\mathbf{b},$$

dove

(1) $\mathbf{a} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $\mathbf{b} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$;

(2) $\mathbf{a} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & -1 \end{pmatrix}$, $\mathbf{b} = \begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix}$.

Esercizio 68. *Calcolare, se possibile, le inverse delle seguenti matrici a coefficienti in $\mathbb{Z}_3$:*

(1) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$;

(2) $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$.

Esercizio 69. *Si dica quali delle seguenti matrici quadrate sono invertibili. Si calcoli l'inversa di quelle invertibili e si determini una matrice X tale che $\mathbf{X}\cdot\mathbf{A} = \mathbf{0}$ per le matrici $\mathbf{A}$ che non sono invertibili.*

(1) $\begin{pmatrix} 1 & 0 \\ 1 & \sqrt{3} \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$ *(Matrici reali);*

(2) $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ *(matrici su $\mathbb{Z}_3$);*

(3) $\begin{pmatrix} 2 & 0 & -1 & 2 \\ 0 & 0 & -1 & 1 \\ -3 & 1 & 0 & 2 \\ 3 & 1 & -1 & 6 \end{pmatrix}$ *(matrice su $\mathbb{Z}_7$).*

Esercizio 70. *Si dica per quali valori di $h \in \mathbb{R}$ la matrice*

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

è invertibile, e se ne determini l'inversa. Si risponda alla domanda considerando invece il campo base $F \in \{\mathbb{Z}_2, \mathbb{Z}_5, \mathbb{Z}_{11}, \mathbb{Z}_{13}\}$ (e di conseguenza $h \in F$).

Esercizio 71. *Calcolare il determinante delle seguenti matrici a coefficienti in $\mathbb{Z}_{11}$:*

(1) $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$;

(2) $\begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}$

(3) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 5 & 2 & 0 & 0 \\ 8 & 6 & 3 & 0 \\ 0 & 9 & 7 & 4 \end{pmatrix}$

(4) $\begin{pmatrix} 1 & 4 & 1 & 3 \\ 2 & 3 & 5 & 0 \\ 4 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{pmatrix}$

(5) $\begin{pmatrix} 1 & 2 & 5 & 6 \\ 3 & 1 & 7 & 7 \\ 0 & 0 & 2 & 3 \\ 4 & 1 & 2 & 5 \end{pmatrix}$.

Esercizio 72. *Sia* $\mathbf{a}_1 := (1) \in M_1(F)$ *e ricorsivamente* $\mathbf{a}_n := \begin{pmatrix} \mathbf{0} & 1 \\ \mathbf{a}_{n-1} & \mathbf{0} \end{pmatrix}$ *per* $n \geqslant 2$. *Si calcoli per induzione su* n *il determinante* $\det(\mathbf{a}_n)$.

Esercizio 73. *Calcolare*

$$\det \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 2 & 3 & \dots & n \\ 3 & 3 & 3 & \dots & n \\ \vdots & & & \ddots & \vdots \\ n & n & n & \dots & n \end{pmatrix}$$

(matrice a coefficienti reali) per ogni $n \geqslant 2$.

Esercizio 74. *Sia* $\mathbf{a} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, *e sia* $f : M_{2\times 1}(\mathbb{R}) \to M_{2\times 1}(\mathbb{R})$ *definita tramite*

$$f : \begin{pmatrix} x \\ y \end{pmatrix} \to \mathbf{a} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

f è iniettiva? E' suriettiva?

Esercizio 75. *Sia* $\mathbf{a} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \in M_2(\mathbb{R})$, *e sia* $f : M_{2\times 1}(\mathbb{R}) \to M_{2\times 1}(\mathbb{R})$ *definita tramite*

$$f : \begin{pmatrix} x \\ y \end{pmatrix} \to \mathbf{a} \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

La funzione f è iniettiva? E' suriettiva?

Esercizio 76. *Si determinino tutte le soluzioni dell'equazione* $x_1+x_2+2x_3-x_4 = 3$ *a coefficienti in* $\mathbb{Z}_{23}$. *Quante sono?*

Esercizio 77. *Si riducano a forma normale le seguenti matrici reali, tenendo traccia delle operazioni elementari effettuate sulle righe:*

(1) $\begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 1 & 3 \end{pmatrix}$;

(2) $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 3 & 1 & 1 & 2 \end{pmatrix}$;

(3) $\begin{pmatrix} 0 & 2 & 1 \\ 0 & 2 & 2 \\ 0 & 2 & 2 \\ 0 & 2 & 1 \end{pmatrix}$;

(4) $\begin{pmatrix} 1 & -1 & \sqrt{2} & 0 \\ 0 & 1 & \sqrt{2} & -1 \\ \sqrt{2} & 0 & -1 & 1 \\ -1 & 2 & 2 & 1 \end{pmatrix}$

Esercizio 78. *Si risolvano i seguenti sistemi lineari su* $F \in \{\mathbb{Q}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}\}$

(1) $\begin{cases} x & & & + & 2z & = & 0 \\ x & - & y & + & 3z & = & 1 \\ & & y & + & 2z & = & -2 \end{cases}$

(2) $\begin{cases} 2x & + & 3y & - & z & = & -3 \\ x & & & + & z & = & 0 \\ x & + & 2y & - & z & = & -2 \end{cases}$

(3) $\begin{cases} & & y & - & z & = & 0 \\ x & & & + & 3z & = & 2 \\ x & + & 3y & + & 2z & = & 2 \\ x & + & 2y & + & z & = & 2 \end{cases}$

Esercizio 79. *Si risolvano i seguenti sistemi lineari omogenei su* $F \in \{\mathbb{Q}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}\}$

(1) $\begin{cases} x & + & 2y & + & 3z & - & t & = & 0 \\ & & y & + & 2z & + & t & = & 0 \\ x & - & y & & & + & 2t & = & 0 \\ x & & & + & 3z & & & = & 0 \end{cases}$

(2) $\begin{cases} x & + & y & + & z & + & t & = & 0 \\ x & + & 2y & + & 3z & - & t & = & 0 \\ x & - & 2y & - & 5z & + & 7t & = & 0 \end{cases}$

Esercizio 80. *Si discutano i seguenti sistemi lineari al variare di* h *in* F*, per* $F \in \{\mathbb{Q}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}\}$*:*

(1) $\begin{cases} hx & + & y & - & 2hz & = & 0 \\ & - & y & + & hz & = & 0 \\ hx & & & + & z & = & 0 \end{cases}$

(2) $\begin{cases} hx & + & y & + & z & + & 2t & = & 0 \\ & & y & - & z & + & ht & = & h \\ hx & & & + & 2z & + & 2t & = & h \\ & & 2y & + & hz & + & 2t & = & 0 \end{cases}$

Esercizio 81. *Si discuta il seguente sistema lineare al variare dei parametri* h, k *nel campo* F*, controllando separatamente i casi* $F = \mathbb{Q}$*,* $F = \mathbb{Z}_2$*,* $F = \mathbb{Z}_3$*,* $F = \mathbb{Z}_5$*.*

$$\begin{cases} kx & - & y & = & -h \\ kx & - & y & = & k-1 \\ kx & + & (h-k)y & = & 1-k \end{cases}$$

Esercizio 82. *Discutere e risolvere, al variare del parametro $\lambda \in \mathbb{Z}_{13}$, il sistema lineare seguente:*

$$\begin{cases} 2(\lambda+1)x_1 & +3x_2 & +\lambda x_3 & = & \lambda+4 \\ (4\lambda-1)x_1 & +(\lambda+1)x_2 & +(2\lambda-1)x_3 & = & 2\lambda+2 \\ (5\lambda-4)x_1 & +(\lambda+1)x_2 & +(3\lambda-4)x_3 & = & \lambda-1 \end{cases}$$

Esercizio 83. *Discutere e risolvere, al variare del parametro $\lambda \in \mathbb{Z}_{17}$, il sistema lineare seguente:*

$$\begin{cases} 2x_1 & +x_2 & +x_3 & = & 2 \\ 3x_1 & -x_2 & +2x_3 & = & 6 \\ x_1 & +2x_2 & +3x_3 & = & 2 \\ 5x_1 & +\lambda x_2 & -x_3 & = & 3\lambda \end{cases}$$

Altri esercizi sono disponibili sul Facchini:

- sulle matrici, da pag. 56 a pag. 58,
- sui determinanti, da pag. 367 a pag. 369

Una trattazione più estesa e generale è disponibile nel capitolo 7 del Delizia–Maj–Longobardi–Nicotera, e sul Johnsonbaugh, Appendix A, pag. 605.