$\mathbb{F}_4$, $\mathbb{Z}/4\mathbb{Z}$ e dintorni...

Abbiamo messo in evidenza l'esistenza di campi di caratteristica 2, quali $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, perché tali campi costituiscono spesso un'eccezione a proprietà valide su tutti gli altri campi. Ad esempio, le *simmetrie* (rispetto a sottospazi vettoriali) sono tutte e sole le applicazioni lineari, $\sigma : V \to V$, tali che $\sigma^2 = id_V$, solo se V è uno spazio vettoriale su un campo C di caratteristica diversa da 2; mentre per spazi vettoriali su campi di caratteristica 2, esistono applicazioni lineari soddisfacenti a quella condizione che non sono simmetrie.

Vogliamo quindi dare qualche maggiore informazione sui campi di caratteristica 2 e, più in generale sui campi finiti. È noto dal corso di Algebra che, per ogni numero primo, p, l'anello $\mathbb{Z}/p\mathbb{Z}$ delle classi resto modulo p, è un campo di caratteristica p e tutti i suoi elementi soddisfano all'*identità di Fermat* $x^p - x = 0$. Talvolta questo campo si indica anche con il simbolo $\mathbb{F}_p$ o GF_p. Più in generale, *è vero che per ogni primo p di $\mathbb{Z}$ e per ogni intero positivo n esiste un campo di caratteristica p, $\mathbb{F}_{p^n}$, che ha esattamente p^n elementi, tutti soddisfacenti all'identità $x^{p^n} - x = 0$. Tale campo è determinato da questa condizione a meno di isomorfismo e, dati due interi positivi, m ed n, $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ se, e solo se, $m \mid n$ (m divide n).*

Non daremo una dimostrazione di questi fatti che richiederebbe tecniche più avanzate di quelle finora introdotte e che esulano dalla materia specifica del corso, che dovrebbe occuparsi di Algebra lineare e Geometria. Ci limitiamo quindi a qualche osservazione ed a qualche esempio legati a questi argomenti.

È noto, sempre dal corso di Algebra, che gli anelli di classi resto $\mathbb{Z}/n\mathbb{Z}$ *non* sono campi quando n non è un numero primo. Si vedano, ad esempio, qui a fianco le tabelle delle operazioni su $\mathbb{Z}/4\mathbb{Z}$ ed è subito evidente che questo anello non ha caratteristica 2 ($1 + 1 = 2 \neq 0$) e non può essere un campo perché $2 \cdot 2 = 0$ e quindi 2 non può essere invertibile (chiarirsi bene questo fatto!).

Operazioni in $\mathbb{Z}/4\mathbb{Z}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Quindi, può essere naturale chiedersi come si possano costruire i campi finiti descritti sopra. Ripetiamo la nostra intenzione di non esporre fatti generali e di limitarci a dare qualche esempio. Gli esempi che proponiamo ricalcano la costruzione dei numeri complessi a partire dai numeri reali: in quel caso si è "aggiunto" ai numeri reali il simbolo i, con $i^2 = -1$, ovvero una radice del polinomio $X^2 + 1$, che non poteva esistere in $\mathbb{R}$.

Il campo $\mathbb{F}_4$ si ottiene aggiungendo ad $\mathbb{F}_2$ un elemento, a, tale che $a^2 = a + 1$, ovvero una soluzione dell'equazione $X^2 + X + 1 = 0$ (*), che non c'è in $\mathbb{F}_2$. Si ottengono così quattro elementi per il campo $\mathbb{F}_4 = \{0, 1, a, a + 1\}$ e le operazioni sono descritte nelle seguenti tabelle.

$+$	0	1	a	$a+1$
0	0	1	a	$a+1$
1	1	0	$a+1$	a
a	a	$a+1$	0	1
$a+1$	$a+1$	a	1	0

$\cdot$	0	1	a	$a+1$
0	0	0	0	0
1	0	1	a	$a+1$
a	0	a	$a+1$	1
$a+1$	0	$a+1$	1	a

In modo perfettamente analogo, il campo $\mathbb{F}_8$ si può ottenere aggiungendo ad $\mathbb{F}_2$ un elemento, b, tale che $b^3 = b + 1$ e riportiamo qui sotto le tabelle delle operazioni per chi sia così pigro da non volerle fare da solo.

$+$	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
0	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
1	1	0	$b+1$	b	b^2+1	b^2	b^2+b+1	b^2+b
b	b	$b+1$	0	1	b^2+b	b^2+b+1	b^2	b^2+1
$b+1$	$b+1$	b	1	0	b^2+b+1	b^2+b	b^2+1	b^2
b^2	b^2	b^2+1	b^2+b	b^2+b+1	0	1	b	$b+1$
b^2+1	b^2+1	b^2	b^2+b+1	b^2+b	1	0	$b+1$	b
b^2+b	b^2+b	b^2+b+1	b^2	b^2+1	b	$b+1$	0	1
b^2+b+1	b^2+b+1	b^2+b	b^2+1	b^2	$b+1$	b	1	0

$\cdot$	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
0	0	0	0	0	0	0	0	0
1	0	1	b	$b+1$	b^2	b^2+1	b^2+b	b^2+b+1
b	0	b	b^2	b^2+b	$b+1$	1	b^2+b+1	b^2+1
$b+1$	0	$b+1$	b^2+b	b^2+1	b^2+b+1	b^2	1	b
b^2	0	b^2	$b+1$	b^2+b+1	b^2+b	b	b^2+1	1
b^2+1	0	b^2+1	1	b^2	b	b^2+b+1	$b+1$	b^2+b
b^2+b	0	b^2+b	b^2+b+1	1	b^2+1	$b+1$	b	b^2
b^2+b+1	0	b^2+b+1	b^2+1	b	1	b^2+b	b^2	$b+1$

(*) Attenzione ché in caratteristica 2, $1 + 1 = 0$ e quindi $1 = -1$.

Invitiamo il lettore a farsi qualche calcolo sul campo $\mathbb{F}_9$, che si può ottenere da $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ aggiungendo una radice del polinomio X^2+1 o sul campo $\mathbb{F}_{25}$, che si può ottenere da $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ aggiungendo una radice del polinomio $X^2 - X + 1$. Che polinomio prendere per $\mathbb{F}_{49}$?

Il lettore più coscenzioso può fare anche altre verifiche, come osservare che $\mathbb{F}_4$ è uno spazio vettoriale su $\mathbb{F}_2$, generato da 1 ed a, così come lo è $\mathbb{F}_8$, con $1, b, b^2$ come base (...e in generale?). Ugualmente, può verificare che anche l'aggiunzione ad $\mathbb{F}_2$ di una radice del polinomio $X^3 + X^2 + 1$ produce un campo di caratteristica 2 con 8 elementi ed è invitato ad esplicitare l'isomorfismo tra questo e quello descritto nelle righe precedenti.

Concludiamo questa parte con l'osservazione che, *per costruire il campo $\mathbb{F}_{p^n}$ è sufficiente aggiungere ad $\mathbb{F}_p$ una radice, t, di un polinomio monico, $P(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n$, irriducibile(*) in $\mathbb{F}_p[X]$ e di grado n.* In tal caso gli elementi $\{1, t, t^2, \ldots, t^{n-1}\}$ generano uno spazio vettoriale di dimensione n su $\mathbb{F}_p$ e la relazione $-a_0 - a_1t - \cdots - a_{n-1}t^{n-1} = t^n$ permette di definire un prodotto sugli elementi di tale spazio che lo rende un campo.

Per trovare un'altra giustificazione del fatto di esserci occupati dei corpi finiti, e per evitare di scrivere enormi tabelle per le operazioni, vogliamo mostrare come si possano usare le matrici per rappresentare gli elementi di un campo finito che può quindi essere identificato con un sottoinsieme di un opportuno anello di matrici, ove le operazioni sono proprio la somma e il prodotto tra matrici.

Cominciamo rivedendo l'esempio del campo dei numeri complessi. È facile verificare che possiamo associare al numero complesso $z = a + ib$, $(a, b) \in \mathbb{R}^2$, la matrice $Z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in M_2(\mathbb{R})$ e che, in tal modo la somma e il prodotto di numeri complessi si trasforma nella somma ed il prodotto delle matrici corrispondenti. Detto in modo più preciso, *l'applicazione $z \mapsto Z$, definita sopra, è un isomorfismo tra il campo dei numeri complessi, $\mathbb{C}$, e il sottoanello di $M_2(\mathbb{R})$,*

$$\mathscr{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid (a, b) \in \mathbb{R}^2 \right\}.$$

Per capire da dove nascano queste matrici il lettore può ragionare come segue. $\mathbb{C}$ è uno spazio vettoriale di dimensione 2 su $\mathbb{R}$, di base $\mathcal{I} = \{1, i\}$ e la moltiplicazione per z è un'applicazione lineare che ha matrice $Z = \alpha_{\mathcal{I},\mathcal{I}}(z)$. In particolare,

$$\alpha_{\mathcal{I},\mathcal{I}}(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \alpha_{\mathcal{I},\mathcal{I}}(i) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \alpha_{\mathcal{I},\mathcal{I}}(a + ib) = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

In modo perfettamente analogo, $\mathbb{F}_4$ è uno spazio vettoriale su $\mathbb{F}_2$, di base $\mathcal{A} = \{1, a\}$. La moltiplicazione per 1 ha matrice $\alpha_{\mathcal{A},\mathcal{A}}(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M_2(\mathbb{F}_2)$ e la moltiplicazione per a ha matrice $\alpha_{\mathcal{A},\mathcal{A}}(a) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{F}_2)$. La moltiplicazione per un generico elemento, $x + ya$ di $\mathbb{F}_4$, con $(x, y) \in \mathbb{F}_2^2$, ha quindi matrice $\begin{pmatrix} x & y \\ y & x+y \end{pmatrix}$ ed $\mathbb{F}_4$ si identifica col sottoanello $\mathscr{F} = \left\{ \begin{pmatrix} x & y \\ y & x+y \end{pmatrix} \mid (x, y) \in \mathbb{F}_2^2 \right\}$, di $M_2(\mathbb{F}_2)$.

Allo stesso modo, $\mathbb{F}_8$, è uno spazio vettoriale su $\mathbb{F}_2$, di base $\mathcal{B} = \{1, b, b^2\}$. La moltiplicazione per gli elementi della base produce le matrici in $M_3(\mathbb{F}_2)$,

$$\alpha_{\mathcal{B},\mathcal{B}}(1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \alpha_{\mathcal{B},\mathcal{B}}(b) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad \alpha_{\mathcal{B},\mathcal{B}}(b^2) = \alpha_{\mathcal{B},\mathcal{B}}(b)^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

La moltiplicazione per un generico elemento, $x + yb + zb^2$ di $\mathbb{F}_8$, con $(x, y, z) \in \mathbb{F}_2^3$, ha quindi matrice $\begin{pmatrix} x & z & y \\ y & x+z & y+z \\ z & y & x+z \end{pmatrix} \in M_3(\mathbb{F}_2)$.

Nel caso del campo $\mathbb{F}_{p^n}$, associato al polinomio monico irriducibile, $P(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in \mathbb{F}_p[X]$, si considera la base $\mathcal{T} = \{1, t, t^2, \ldots, t^{n-1}\}$. La matrice identica $\mathbf{1}_n$, la matrice $T = \alpha_{\mathcal{T},\mathcal{T}}(t) \in M_n(\mathbb{F}_p)$ [scriverla!] e le sue potenze, $T^2, \ldots, T^{n-1}$ permettono di costruire un sottocampo di $M_n(\mathbb{F}_p)$ isomorfo al campo $\mathbb{F}_{p^n}$. Invitiamo il lettore a sviluppare per proprio conto un po' di esempi di questa costruzione.

(*) *Non basta che non vi siano radici del polinomio in $\mathbb{F}_p$; è necessario che $P(X)$ non si possa scrivere come prodotto di due polinomi di grado strettamente più piccolo in $\mathbb{F}_p[X]$.*