In generale B_n, l'insieme dei polinomi in n variabili $x_1, \ldots, x_n$ codifica le funzioni da W^n, il prodotto cartesiano di n copie di W in W. La sua cardinalità vale 2^{2^n} ed i suoi elementi sono somme di monomi della forma

$$x_{i_1} \cdots x_{i_k}, 1 \leq i_1 < \ldots < i_k \leq n, 0 \leq k \leq n$$

(se k vale 0 si ha il polinomio costantemente uguale a 1).

Vediamo in dettaglio un esempio più concreto. Nel Tema d'Esame del Giugno 2023 viene chiesto di stabilire la natura della seguente formula in tre variabili proposizionali

$$\neg((s \vee \neg t) \to (t \vee q)) \vee (s \to (t \vee q)).$$

Ne viene fornita una soluzione tramite le tavole di verità. Noi traduciamo invece il problema in termini matematici/polinomiali e calcoliamo.

1.3 Magma

Possiamo affrontare il problema con carta e penna ma ritengo sia più proficuo utilizzare un programma di manipolazione simbolica tra quelli menzionati. Per varie ragioni preferisco utilizzare Magma. Inizio ad implementare le funzioni negazione, disgiunzione e implicazione. Quest'ultima vale $\neg p \vee q$, ossia

$$(1 + x) + y + (1 + x)y = 1 + x + y + y + xy = 1 + x + xy.$$

La sintassi in Magma è abbastanza autoesplicativa:

```
neg:=func<x|1+x>;
vel:=func<x,y|x+y+x*y>;
imp:=func<x,y|1+x+x*y>;
```

L'insieme dei coefficienti $W = B_0$ costituisce un esempio di **campo**, un analogo minimale dell'insieme dei numeri reali, dei numeri complessi o dei razionali; esempi che sicuramente avete incontrato in nel carso di Algebra Lineare. Questo è il primo esempio di una famiglia doppiamente infinita di campi aventi cardinalità finita detti campi di Galois (GF o Galois Fields). Su questi coefficienti costruiamo l'anello dei polinomi in tre variabili:

```
F:=GF(2);
A:=PolynomialRing(F,3);
```

Mentre la condizione $2p = 0$ è già codificata in queste istruzioni, dobbiamo imporre che $x^2 = x$ per ogni variabile. A tal fine si deve costruire una struttura **quoziente** introducendo un'opportuna **relazione di equivalenza**. Questo concetto è stato già introdotto l'anno scorso quindi non darò per scontato che sappiate cosa è una relazione di equivalenza.

```
B<s,t,q>,bb:=quo<A|[A.i^2-A.i:i in [1..Rank(A)]]>;
```

Definizione 3.16 *Sia X un insieme su cui è definita un'operazione binaria $*$ e una relazione d'equivalenza R. Si dice che R è compatibile con l'operazione $*$, o che R è una* ***congruenza*** *rispetto all'operazione $*$, se $\forall a, a', b, b' \in X$*

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

Lemma 3.17 *Mostriamo che R è una congruenza rispetto $a *$ sse $\forall a, b, c \in X$ aRb implica $(a * c)R(b * c)$ e $(c * a)R(c * b)$.*

Dim. Sia R una congruenza e aRb. Siccome cRc, si ha sia $a * cRb * c$ che $c * aRc * b$. Viceversa siano aRb e $a'Rb'$, allora $(a * a')R(b * a')$ e $(b * a')R(b * b')$, da cui per transitività $(a * a')R(b * b')$. □

Definizione 3.18 *Indichiamo per $a \in X$ con $[a]_R$ la classe di equivalenza $\{b \in X : bRa\}$ di a rispetto ad R e con $X/R = \{[a]_R : a \in X\}$ l'insieme quoziente.*

Proposizione 3.19 *Sia R una congruenza su un insieme X dotato dell'operazione $*$, allora è definita su X/R l'operazione $*_R : X/R \times X/R \to X/R$ ponendo $\forall\ [a]_R, [b]_R \in X/R$:*

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

Dim. Dimostriamo che tale operazione è ben definita modificando i rappresentanti delle classi coinvolte. Sia aRa', allora $(a * b)R(a' * b)$. Si procede analogamente se $b'Rb$. □

L'importanza di questa proposizione è che fornisce una ricetta per costruire nuove strutture algebriche a partire da congruenze su strutture note.

3.4 Congruenze sugli interi

Sia $\mathbb{N} = \{0, 1, 2, \ldots\}$ l'insieme dei numeri naturali (in questo corso $0 \in \mathbb{N}$). Nel corso di Fondamenti avete incontrato la nozione di relazione di equivalenza. Il concetto di congruenza ottenuta da una relazione rispetto ad un'operazione è originato dalle congruenze su $\mathbb{Z}$. Queste sono state introdotte da Gauss agli inizi dell'Ottocento per risolvere varie questioni di Teoria dei Numeri.

Definizione 3.20 *Siano $a,\ b \in \mathbb{Z}$. Si dice che b* ***divide*** *a (o a è un* ***multiplo*** *di b) e si scrive $b \mid a$ se esiste $c \in \mathbb{Z}$ tale che $a = bc$. Dato $m \in \mathbb{N}$, si dice b^m è la massima potenza di b che divide a se $b^m \mid a$ ma $b^{m+1} \nmid a$. Si scriverà anche $b^m \mid\mid a$.*

Osservazione 3.21 *Si osservi che la relazione aRb sse $a \mid b$ è riflessiva e transitiva, ma non simmetrica. Se $a \mid b$ e $b \mid a$, allora $b = \pm a$.*

Definizione 3.22 *Sia $n \in \mathbb{Z},\ n > 1$. Se $a,\ b \in \mathbb{Z}$ diciamo che a è* ***congruo*** *b modulo n e scriviamo*

$$a \equiv b \pmod{n} \qquad \text{o} \qquad a \equiv_n b$$

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

Un esempio di risultato che coinvolge le congruenze è il seguente:

Teorema 3.23 (Piccolo Teorema di Fermat) *Sia p primo e $a \in \mathbb{Z}$ con $p \nmid a$. Allora $a^{p-1} \equiv 1 \pmod{p}$.*

Si noti che $a \equiv b \pmod{n}$ sse $a \equiv b \pmod{-n}$. Inoltre per $n = 0$, $a \equiv b \pmod{n}$ sse $a = b$. Quindi possiamo d'ora in poi assumere $n > 0$.

Proposizione 3.24 *La relazione di congruenza modulo n è di equivalenza. Se $n > 0$, le partizioni determinate dalle classi di equivalenza sono esattamente n. Indicata con $[\,a\,]_n$ la classe di equivalenza contenente a, l'insieme delle classi di equivalenza fissato n sono $[\,0\,]_n$, $[\,1\,]_n$, $\ldots, [\,n-1\,]_n$; sono cioè rappresentate da tutti i possibili resti nella divisione intera per n.*

Dim. Proviamo che è una relazione di equivalenza.

1. Riflessiva: Infatti $a - a = 0n$.
2. Simmetrica: $a - b = hn$ implica $b - a = (-h)n$.
3. Transitiva: $a - b = hn$ e $b - c = kn$ implica $a - c = (h + k)n$.

Sia $a = nq + r$, con $0 \leq r < n$, allora $a \equiv r \pmod{n}$. Infine se $0 \leq r \leq s < n$, allora $s \equiv r \pmod{n}$ sse $r = s$. Quindi ho esattamente n classi di equivalenza rappresentate da $0 \leq r < n$. □

Definizione 3.25 *Sia $\mathbb{Z}$ con la relazione $\equiv_n$ di congruenza modulo n. Allora le classi $[\,a\,]_n$ vengono dette classi di resto e l'insieme quoziente viene indicato con*

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

Facciamo notare che gli interi tra 0 e $n-1$ non sono gli unici rappresentanti per le classi di resto. Per vari motivi sono importanti anche rappresentanti s piccoli in valore assoluto, ossia tali che $|2s| \leq n$.

Definizione 3.26 *Dato $0 < n \in \mathbb{N}$ e la relazione di congruenza modulo n, si dicono **rappresentanti canonici** gli interi r tali che $0 \leq r < n$, ossia i resti della divisione mediante n. Si dicono **rappresentanti ridotti** gli interi s tali che $2|s| \leq n$ e se $n = 2m$ è pari, essendo m e $-m$ equivalenti, si pone m come rappresentante ridotto della classe $[m]_n$.*

Esercizio 3.27 *Mostrare che i rappresentanti ridotti modulo $0 < n \in \mathbb{N}$ si possono definire come gli interi tali che*

$$-\frac{n-1}{2} \leq s \leq \frac{n}{2}$$

(distinguete i casi n pari, dispari).

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

Proposizione 3.28 *La congruenza modulo n è compatibile con $+$ e $\cdot$ definiti in $\mathbb{Z}$.*

Dim. Bisogna provare la compatibilità con somma e prodotto, ossia dobbiamo provare che

$$a \equiv a',\ b \equiv b' \pmod{n} \implies (a+b) \equiv (a'+b'),\ ab \equiv a'b' \pmod{n}.$$

Le prime due condizioni implicano che esistono $h, k \in \mathbb{Z}$ tali che:

$$a - a' = hn, b - b' = kn.$$

Da queste ricaviamo $a = a' + hn$ e $b = b' + kn$. Quindi

$$a + b = a' + b' + (h+k)n.$$

e

$$ab = a'b' + (hb' + ka' + hkn)n,$$

da cui $a' + b' \equiv a + b,\ a'b' \equiv ab \pmod{n}$. □

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

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

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

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

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

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

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

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

Esempio 3.29 *Poniamo $n = 6$ e scriviamo le tavole di composizione della somma e del prodotto in $\mathbb{Z}/6$. Per comodità di scrittura si scriverà $\boldsymbol{k}$ invece di $[\,k\,]_6$, il lettore presti attenzione a questo particolare in modo da non confondere $[\,k\,]_6$ con il valore k.*

Dalla tavola di composizione della somma si può trovare l'inverso di un elemento di $\mathbb{Z}/6$ semplicemente scorrendo la riga e cercando l'unità (cioè lo $\mathbf{0}$). Ad esempio si ha che $\mathbf{4}+\mathbf{2} = \mathbf{0}$ ($[\,4\,]_6 + [\,2\,]_6 = [\,0\,]_6$) e quindi $\mathbf{4}$ è inverso sinistro (e bilatero, per la commutatività) di $\mathbf{2}$. Osservando la tavola di composizione del prodotto si nota facilmente che non tutti gli elementi hanno inverso! Infatti

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

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

non in tutte le righe e colonne compare l'unità del prodotto. Se si osserva attentamente quali elementi hanno un inverso si scopre che solo **1** e **5** hanno inverso (bilatero). È interessante notare che tali elementi sono gli unici **coprimi** con il valore 6. Sono gli unici x tale che $\mathrm{MCD}(x, 6) = 1$. Questa caratteristica in realtà vale in generale.

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

Proposizione 3.30 *Sia* $ax \equiv b \pmod{n}$ *una congruenza lineare modulo* n*. Allora tale congruenza ha soluzioni se e solo se* $\mathrm{MCD}(a, n) \mid b$*. In particolare* a *ammette inverso modulo* n *se e solo se* $\mathrm{MCD}(a, n) = 1$*.*

Esempio 3.31 *Se consideriamo la congruenza modulo* 5 *possiamo subito prevedere che ogni elemento non nullo di* $\mathbb{Z}/5$ *ammette inverso rispetto al prodotto in tale insieme.*

Infatti le tavole di composizione su $\mathbb{Z}/5$ sono:

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

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

E questa volta in ogni riga e colonna (**0** escluso) compare un **1**, come previsto. Inoltre l'insieme così costruito eredita da $\mathbb{Z}$ tutte le proprietà e in definitiva è possibile verificare che $(\mathbb{Z}/5, +, \cdot)$ è un **campo**.

Dati $a, b, c \in \mathbb{Z}$, l'equazione $ax + by = c$ da risolvere in $\mathbb{Z}$ è uno dei primi esempi di **equazioni diofantee**. Come vedremo la restrizione di determinare solo le soluzioni intere rende molto più complessa la risoluzione. Supponiamo per esempio di dover risolvere l'equazione $2x - 5y = 3$. Possiamo riscrivere allora l'equazione come $2x - 3 = 5y$, che equivale a dire $5 \mid (2x - 3)$, che avviene se $2x \equiv 3 \pmod{5}$. Passando allora da $\mathbb{Z}$ a $\mathbb{Z}/5$ possiamo risolvere l'equazione con quanto visto

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

Cioè le soluzioni sono della forma $x = 4 + 5k$ al variare di $k \in \mathbb{Z}$.

Esercizio 3.32 *Scrivere codice in* Magma *in grado di determinare il giorno della settimana di una certa data. Attenzione alle regole per il calcolo degli anni bisestili. Cercare in rete la presenza di algoritmi all'uopo ideati.*

3.5 Congruenze sui polinomi

In modo analogo si possono definire congruenze in $A = K[x]$.

Definizione 3.33 *Dati n, a in A si dice che n divide a se esiste $b \in A$ tale che $a = nb$ e scriveremo $n|a$.*

Si fissi $n = n(x) \in A$ e si definisca aE_nb sse $n|a - b$.

Esercizio 3.34 *Dimostrare che E_n definisce una relazione di equivalenza su A.*

Esempio 3.35 *Se $n = 0_A$, il polinomio nullo, allora $n|a - b$ sse esiste $c \in A$ tale che $a - b = 0_A c = 0_A$, cioè $a = b$.*

Sia $a \in K$, allora possiamo pensare ad a come il polinomio costante

$$a \cdot 1_A + 0 \cdot x + \cdots .$$

Notate che scrivo $0_A, 1_A$ per sottolineare che si tratta del polinomio nullo e identicamente uguale a 1 (questo senza indice A perché trattasi di 1_K).

Esempio 3.36 *Sia $0_K \neq n \in K$ e $a \in A$, allora $a = n \cdot n^{-1}a$, ossia n divide qualsiasi polinomio. Quindi aE_n0_a per ogni $a \in A$.*

Analizziamo cosa accade quando n è un polinomio di grado positivo $d > 0$. Dato $a \in A$, l'algoritmo di divisione lunga afferma che esistono $q, r \in A$ tali che $a = nq + r$, $\deg(n) < d$, ossia $n|a - r$. Quindi aE_nr. Sia $r' \in A$ con $\deg(r') < d$ e aE_nr'. Allora rE_nr' e n divide $r' - r$. Avendo grado minore di d, si ha $r = r'$. Abbiamo quindi

Teorema 3.37 *Dato $n \in A$ di grado $d > 0$, si ponga $E = E_n$, allora ogni classe di equivalenza $[a]_E$ contiene uno ed un solo polinomio di grado minore di d.*

Replicando la dimostrazione nel caso degli interi si verifica che E_n è una congruenza sia rispetto alla somma che al prodotto di polinomi. Come abbiamo fatto con gli interi scriveremo $[a]_n$ per la classe di a e $a \equiv_n b$ invece di aE_nb.