QUÈ HEM FET FINS ARA?

A la classe anterior el que vam treballar són els darrers conceptes sobre funcions inclosa la composició de funcions.

CLASSE D'AVUI 23/11/2020

Avui treballarem el que ens queda de composició de funcions i començarem el tema de divisibilitat.

EX.: (43) Calculeu les composicions $g \circ f$ en els casos següents. Es pot calcular $f \circ g$? Amb $f : \mathbb{R} \to \mathbb{R}$ definida per $f(x) = x + 1$, $g : \mathbb{R} \to \mathbb{R}$ definida per $g(x) = x^2$.

Els dominis i conjunts d'arribada són els necessaris per fer la composició. Calculem: $(g \circ f)(x) = g(f(x)) \;\; = g(x+1) = (x+1)^2$.

I amb l'altra composició: $(f \circ g)(x) = f(g(x)) \;\; = f(x^2) = x^2 + 1$. S'observa que la composició no és commutativa.

EX.: (44) Idem amb $f : \mathbb{Z} \to \mathbb{N}$ definida per $f(x) = x \bmod 5$, $g : \mathbb{N} \to \mathbb{R}$ definida $g(x) = \ln(x+1)$.

Els dominis i conjunts d'arribada són els necessaris per fer la composició. Calculem: $(g \circ f)(x) = g(f(x)) \;\; = g(x \bmod 5) = ln(x \bmod 5 + 1)$.

Per l'altra composició els dominis i conjunts d'arribada no són els necessaris per fer la composició. Si ens mirem només les fórmules i "intentem" fer la composició veureu que podria tenir sentit er alguns valor concrets de x però que en general donaria una funció que no estaria ben definida (és a dir, no seria una funció).

Destaquem les principals propietats de la composició de funcions:

PROP.:

1. Associativa: si $f : A \to B$, $g : B \to C$, $h : C \to D$ llavors $h \circ (g \circ f) = (h \circ g) \circ f$.
2. Si $f : A \to B$, llavors $I_B \circ f = f \circ I_A = f$.
3. La composició de funcions injectives és injectiva.
4. Si $g \circ f$ és injectiva llavors f és injectiva.
5. La composició de funcions exhaustives és exhaustiva.
6. Si $g \circ f$ és exhaustiva llavors g és exhaustiva.
7. La composició de funcions bijectives és bijectiva.
8. Si $g \circ f$ és bijectiva llavors f és injectiva i g és exhaustiva.
9. Si $f : A \to B$ és bijectiva, llavors $f^{-1} \circ f = I_A, f \circ f^{-1} = I_B$.
10. Si $f : A \to B$ i $g : B \to A$ satisfan $g \circ f = I_A$ i $f \circ g = I_B$, llavors les dues són bijectives i cada una és la inversa de l'altra: $g = f^{-1}$ i $f = g^{-1}$.

DEM.: (47) Demostrem 2: $(f \circ I_A)(x) = f(I_A(x)) \;\; = f(x)$ per tant $f \circ I_A = f$. Per l'altra composició fem el mateix: $(I_B \circ f)(x) = I_B(f(x)) \;\; = f(x)$

Demostrem 3: suposem que f i g són injectives i demostrem que la composició també ho és: siguin x, x' pels quals

$(g \circ f)(x) = (g \circ f)(x') \Rightarrow g(f(x)) = g(f(x')) \Rightarrow f(x) = f(x') \Rightarrow x = x'$

per tant és injectiva.

(47) Demostrem 5: suposem que f i g són exhaustives i demostrem que la composició també ho és: donat $c \in C$ busquem un $a \in A$ tal que $(g \circ f)(a) = c \Leftrightarrow g(f(a)) = c$. Per trobar aquest element a utilitzarem les dues exahustivitats. Com que g és exahustiva sabem que existeix un $b \in B$ tal que $g(b) = c$. Ara com que la f també és exahustiva sabem que existeix un $a' \in A$ tal que $f(a') = b$. I per tant: $g(f(a')) = g(b) = c$. Aleshores l'element a que buscàvem és a'. Per tant és exahustiva.

(47) Demostrem 7: per les propietats 3 i 5 surt.

Demostrem 10: que f i g són bijectives surt de les propietats 4 i 6 ja que les identitats són bijectives. Veiem ara que $f = g^{-1}$. Sigui $x \in A$ qualsevol, hem de veure que $g^{-1}(x) \overset{???}{=} f(x)$ cosa que és certa perquè $g(f(x)) = x$ per hipòtesi. De la mateixa manera per un $x \in B$ qualsevol, hem de veure que $f^{-1}(x) = g(x)$ cosa que és certa perquè $f(g(x)) = x$ per hipòtesi.

EX.: (48) Siguin $f : A \to B$, $g : B \to B$ amb f exhaustiva i satisfent $g \circ f = f$. Demostreu que $g = I_B$.

Pista: heu d'intentar demostrar que $g(x) = x$ per $x \in B$. Només cal que considereu un antiimatge de x per f. També surt aplicant el problema 49 (el següent).

EX.: (49) Si $f \circ h = g \circ h$ i h és exhaustiva llavors $f = g$.

Per demostrar que $f = g$ només cal veure que $f(x) \overset{???}{=} g(x)$ per a tot x. Com que h és exhaustiva llavors existeix un x' tal que $h(x') = x$ i llavors en el càlcul de $f(x)$ podem fer: $f(x) = f(h(x')) = g(h(x')) = g(x)$ com volíem demostrar.

EX.: (50) Sigui $f : A \to A$ que satisfà $f \circ f = f$. Demostreu que són equivalents:

a. f és injectiva.

b. f és exhaustiva.

c. f és bijectiva.

d. $f = I_A$.

Veiem les 4 implicacions:

a.$\Rightarrow$**b.** Suposem que f és injectiva i provem que f és exhaustiva. Sigui $y \in A$ i busquem un $x \in A$ tal que $f(x^{???}) = y$. Per la hipòtesi tenim que $f(f(y)) = f(y)$ i per la injectivitat de f tenim que $f(y) = y$ i ja tenim qui pot ser x: la pròpia y.

b.$\Rightarrow$**c.** Suposem que f és exhaustiva i provem que f és injectiva (i per tant serà bijectiva). Suposem que tenim $f(x) = f(x')$ i com que f és exhaustiva llavors tenim uns $a, a' \in A$ tals que $f(a) = x$, $f(a') = x'$. Per tant a partir de $f(x) = f(x')$ podem fer: $f(x) = f(x') \Rightarrow f(f(a)) = f(f(a')) \Rightarrow f(a) = f(a') \Rightarrow x = x'$.

c.$\Rightarrow$**d.** Si f és bijectiva sabem que existeix f^{-1} i llavors:

$f \circ f = f \Rightarrow f^{-1} \circ f \circ f = f^{-1} \circ f \Rightarrow I_A \circ f = I_A \Rightarrow f = I_A$

d.$\Rightarrow$**a.** Si suposem que $f = I_A$ aleshores f és injectiva, per tant queda demostrat a.

EX.: (51) Siguin $f : A \to B$, $g : B \to A$ satisfent $g \circ f = I_A$.
a. Demostreu que si f és exhaustiva llavors $f \circ g = I_B$.
b. Demostreu que si g és injectiva llavors $f \circ g = I_B$.
c. Doneu un exemple on $f \circ g \neq I_B$.

a. Sabem que $g \circ f = I_A$ per tant per les propietats 4 i 6 com que I_A és exhaustiva i injectiva podem concloure que g és exahustiva i que f injectiva. Com que ens dieuen que f és exhaustiva llavors serà bijectiva i per tant exisitirà la inversa f^{-1}:
$g \circ f = I_A \Rightarrow g \circ f \circ f^{-1} = I_A \circ f^{-1} \Rightarrow g = f^{-1}$
i llavors el càlcul següent és molt fàcil: $f \circ g = f \circ f^{-1} = I_B$.
b. Es fa de la mateixa manera.
c. Pel que hem vist als apartats anteriors ha de ser f no exhaustiva i g no injectiva amb $g(f(x)) = x$. Per exemple poden ser: $f : \{1,2\} \to \{1,2,-1\}$, $g : \{1,2,-1\} \to \{1,2\}$ donades per $f(x) = |x|, g(x) = |x|$.

5.-DIVISIBILITAT

En aquest capítol estudiarem a fons el concepte de divisibilitat tot i que ja l'hem utilitzat en temes anteriors.

DEF.: Donats $a,b \in \mathbb{Z}$ direm que $a|b \Leftrightarrow$ existeix $q \in \mathbb{Z}$ tal que $b = aq$
De la mateixa manera diem que b és un múltiple de a o que b és un divisor de a.

EX.: Dieu si són certes o falses les afirmacions següents: $3|6$, $6|3$, $121|121$, $-1|1$, $1|-1$, $3|0$, $0|3$, per a tot enters a,b: $a|b \Leftrightarrow \frac{b}{a} \in \mathbb{Z}$.
És molt fàcil: $3|6$ veritat, $6|3$ fals, $121|121$ veritat, $-1|1$ veritat, $1|-1$ veritat, $3|0$ veritat, $0|3$ fals, per a tot enters a,b: $a|b \Leftrightarrow \frac{b}{a} \in \mathbb{Z}$ fals (contraexemple $a = 0, b = 0$).

Aquesta relació satisfà les propietats:
PROP.: Per a tot $a,b,c,u,v \in \mathbb{Z}$:

1. $1|a$.
2. $a|0$.
3. $a|ab$.
4. Reflexiva: $a|a$.
5. Transitiva: $a|b, b|c \Rightarrow a|c$.
6. $a|b \Rightarrow ac|bc$.
7. Simplificació: si $c \neq 0$ i $ac|bc \Rightarrow a|b$.
8. $a|b \Rightarrow a|bc$.

9. No depèn del signe: $a|b \Leftrightarrow a|-b \Leftrightarrow -a|b \Leftrightarrow -a|-b \Leftrightarrow |a| \mid |b|$

10. Si $b \neq 0$ i $a|b \Rightarrow |a| \leq |b|$.

11. $a|b$ i $b|a \Rightarrow |a| = |b|$.

12. Linealitat: $a|b$ i $a|c \Rightarrow a|ub + vc$.

DEM.: (1) Demostrem 1: $a = 1 \cdot a$.
(1) Demostrem 4: $a = a \cdot 1$.
Demostrem 10: Suposem que $b \neq 0$ i $b = ka \Rightarrow |b| = |k| \cdot |a|$ com $|k| \neq 0$ (si fos nul seria $b = 0$ i no és possible) llavors $|k| \geq 1$ i per tant $|b| \geq |a|$.

EX.: (2) Demostreu que si $a|a + b$ llavors $a|b$.
Molt fàcil: $a|a + b \Leftrightarrow a + b = ka$ per cert k enter $\Rightarrow b = (k - 1)a$ o sigui $a|b$.

EX.: (3) Demostreu que les úniques solucions enteres de l'equació $xy = x + y$ són $x = y = 0$, $x = y = 2$. Pista: proveu que x, y es divideixen mútuament i useu la propietat 11.
Seguint la indicació:
$xy = x + y \Rightarrow y = (y - 1)x \Rightarrow x|y$

$xy = x + y \Rightarrow x = (x - 1)y \Rightarrow y|x$
Ara per la propietat 11 tenim que $|x| = |y| \Rightarrow y = \pm x$. Per tant si $y = x$ l'equació inicial quedarà $xx = x + x \Rightarrow x^2 = 2x \Rightarrow x = \begin{cases} 0 \Rightarrow y = 0 \\ 2 \Rightarrow y = 2 \end{cases}$.
I en el cas que $y = -x$ quedarà $-xx = x - x \Rightarrow -x^2 = 0 \Rightarrow x = 0 \Rightarrow y = 0$.

EX.: (4) Demostreu que si $x|y$ i $y|2x$ llavors o bé $y = \pm x$ o bé $y = \pm 2x$.
Si existeixen enters k, k' tals que: $y = kx$, $2x = k'y \Rightarrow 2x = k'kx$ aleshores distingirem dos casos, $x = 0$ o bé $x \neq 0$. Si $x = 0$ llavors $y = 0$, $k'y = 0$ o sigui $y = 0$ que satisfan les dues condicions. Si $x \neq 0$ llavors $kk' = 2$, per tant $(k, k') = (1, 2), (-1, -2), (2, 1), (-2, -1)$ que ens dona les possibilitats: 1)$y = x$, $2x = 2y$ o sigui $y = x$; 2)$y = -x$, $2x = -2y$ o sigui $y = -x$; 3)$y = 2x$, $2x = y$ o sigui $y = 2x$; 4)$y = -2x$, $2x = -y$ o sigui $y = -2x$.

Un concepte molt important és el de nombre primer:
DEF.: p és primer $\Leftrightarrow p \geq 2$ i els únics divisors positius de p són 1 i p. Quan un nombre (més gran gran que 1) no és primer diem que és compost.
Tenen, entre d'altres, aquestes propietats:
PROP.:

1. Tot nombre enter $n \geq 2$ és primer o és un producte de nombres primers.

2. Tot nombre enter $n \geq 2$ té algún divisor primer p. Si a més n no és primer, podem triar algun divisor primer $p \leq \sqrt{n}$.

3. Hi ha infinits nombres primers.

DEM.: $\varnothing$

El següent concepte important és el de màxim comú divisor:

DEF.: Pels nombres $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ anomenem $mcd(a_1, a_2, \ldots, a_n) = 0$ si $a_1 = a_2 = \ldots = a_n = 0$ i serà $mcd(a_1, a_2, \ldots, a_n) = d$ l'unic nombre enter amb les propietats següents:

- $d|a_i$ per a cada $i = 1, 2, \ldots, n$
- $d'|a_i$ per a cada $i = 1, 2, \ldots, n$ aleshores $d' \leq d$.

Per la definició és immediat que $mcd(a_1, a_2, \ldots, a_n) \geq 0$ i que $mcd(a_1, a_2, \ldots, a_n) = 0$ només en el cas que tots els nombres siguin 0.

Com a propietats importants del màxim comú divisor tenim:

PROP.: Siguin $a, b, p \in \mathbb{Z}$.

1. Si $a|b$ llavors $mcd(a,b) = |a|$.
2. $mcd(a,0) = |a|$.
3. Si p és primer i no divideix b, llavors $mcd(p,b) = 1$.
4. El màxim comú divisor no depèn del signe: $mcd(a,b) = mcd(a,-b) = mcd(-a,b) = mcd(-a,-b)$.
5. Teorema d'Euclides: $mcd(a,b) = mcd(a+ub,b)$.

DEM.: Demostració de 5: només cal demostrar que $mcd(a,b) = mcd(a \pm b, b)$ i després iterant aquesta propietat s'obté la 5:

$mcd(a,b) = mcd(a+b,b) = mcd(a+2b,b) = mcd(a+3b,b) = \ldots = mcd(a+ub,b)$

si $u > 0$ i de la mateixa manera si és negatiu amb $mcd(a,b) = mcd(a-b,b)$. I per justificar $mcd(a,b) = mcd(a+b,b)$ només cal observar que tenen els mateixos divisors:

$c|a, c|b \Rightarrow^{???} c|a+b, c|b$

cert perquè $a = kc, b = k'c \Rightarrow a+b = kc+k'c = (k+k')c$. I a l'inrevés:

$c|a+b, c|b \Rightarrow^{???} c|a, c|b$

també cert perquè $a+b = kc, b = k'c \Rightarrow a+k'c = kc \Rightarrow a = (-k'+k)c$.

El teorema d'Euclides ens obre la porta a trobar una manera de calcular el màxim com divisor d'una manera molt eficient computacionalment parlant ja que les altres vies són molt costoses computacionalment. Veiem en un exemple:

EX.: Calculeu el $mcd(50,16)$ utilitzant la propietat 5.

Podem fer el següent:

$$mcd(50,16) = mcd(50-16,16) = mcd(34,16) = mcd(34-16,16) =$$

$$= mcd(18,16) = mcd(18-16,16) = mcd(2,16) = \ldots$$

Seria molt més fàcil restar al nombre 50 el número més gran de 16s de cop per la qual cosa utilitzo la divisió entera que vam aprendre a l'escola:

50	16
2	3

$\rightarrow mcd(50,16) = mcd(50 - 3 \cdot 16, 16) = mcd(2,16) = mcd(16,2) = \ldots$

16	2
0	8

$\rightarrow \ldots = mcd(16,2) = mcd(16-2 \cdot 8, 2) = mcd(0,2) = 2$

Aquest raonament se sistematitza en una taula com la següent en la qual els quocients es posen per sobre del divisor i el residu passa a ser el nou divisor en cada pas:

	3	8
50	16	2
2	0	

$\rightarrow mcd(50,16) = 2$

EX.: Procediu com a l'exemple anterior per calcular el $mcd(122,54)$.
Seguïm l'esquema:

	2	3	1	6
122	54	14	12	2
14	12	2	0	

$\rightarrow mcd(122,54) = 2$