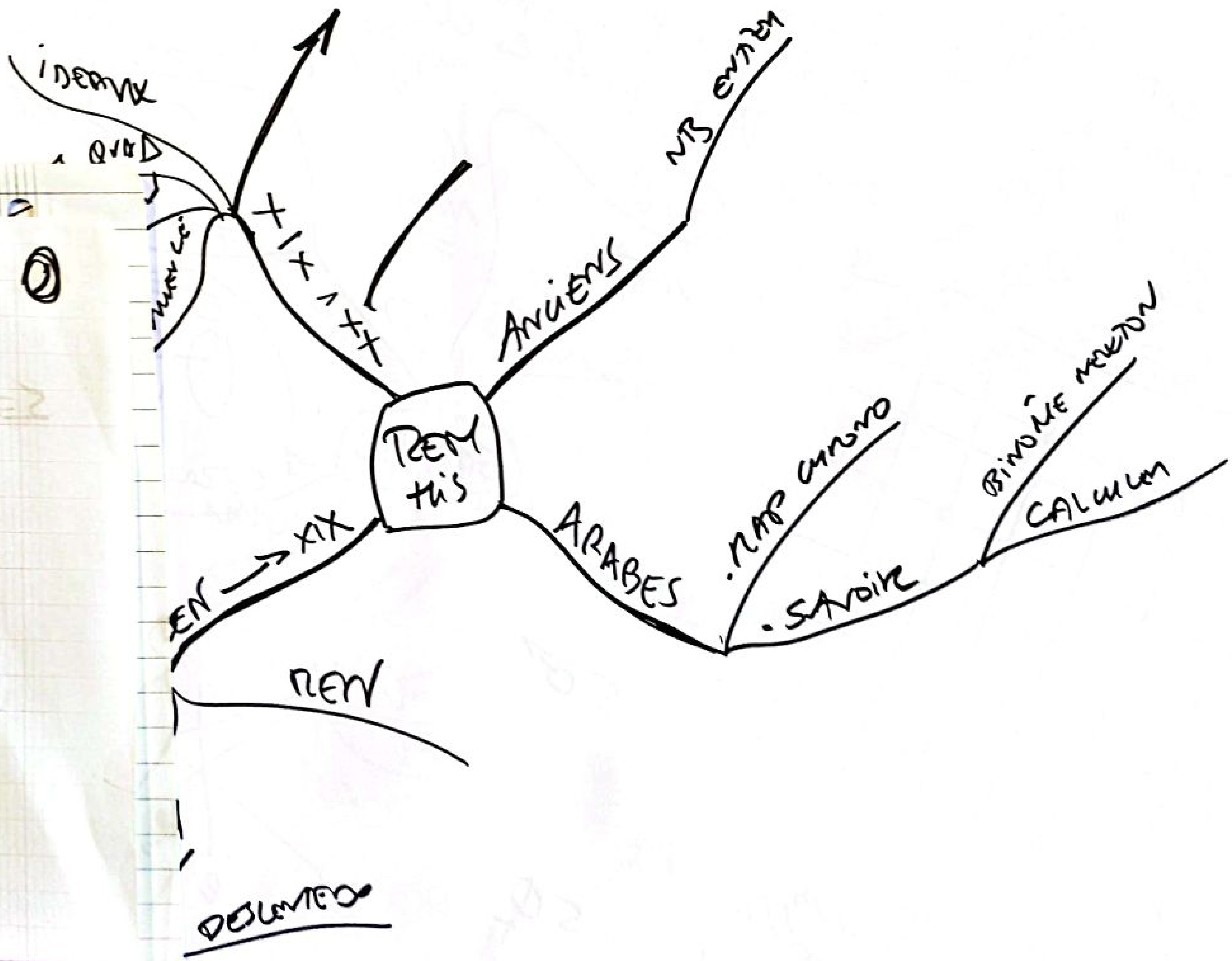
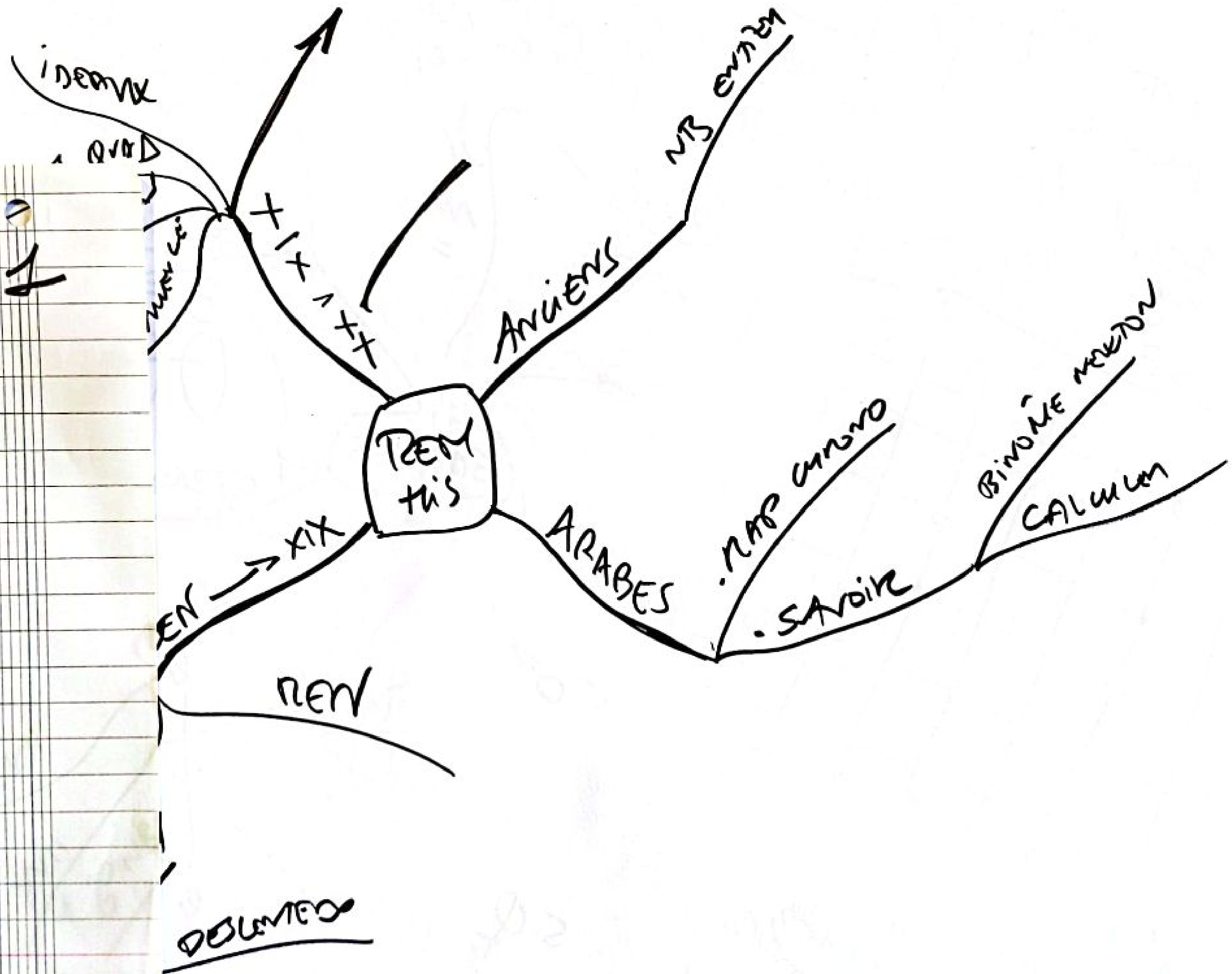
7x40
/
47

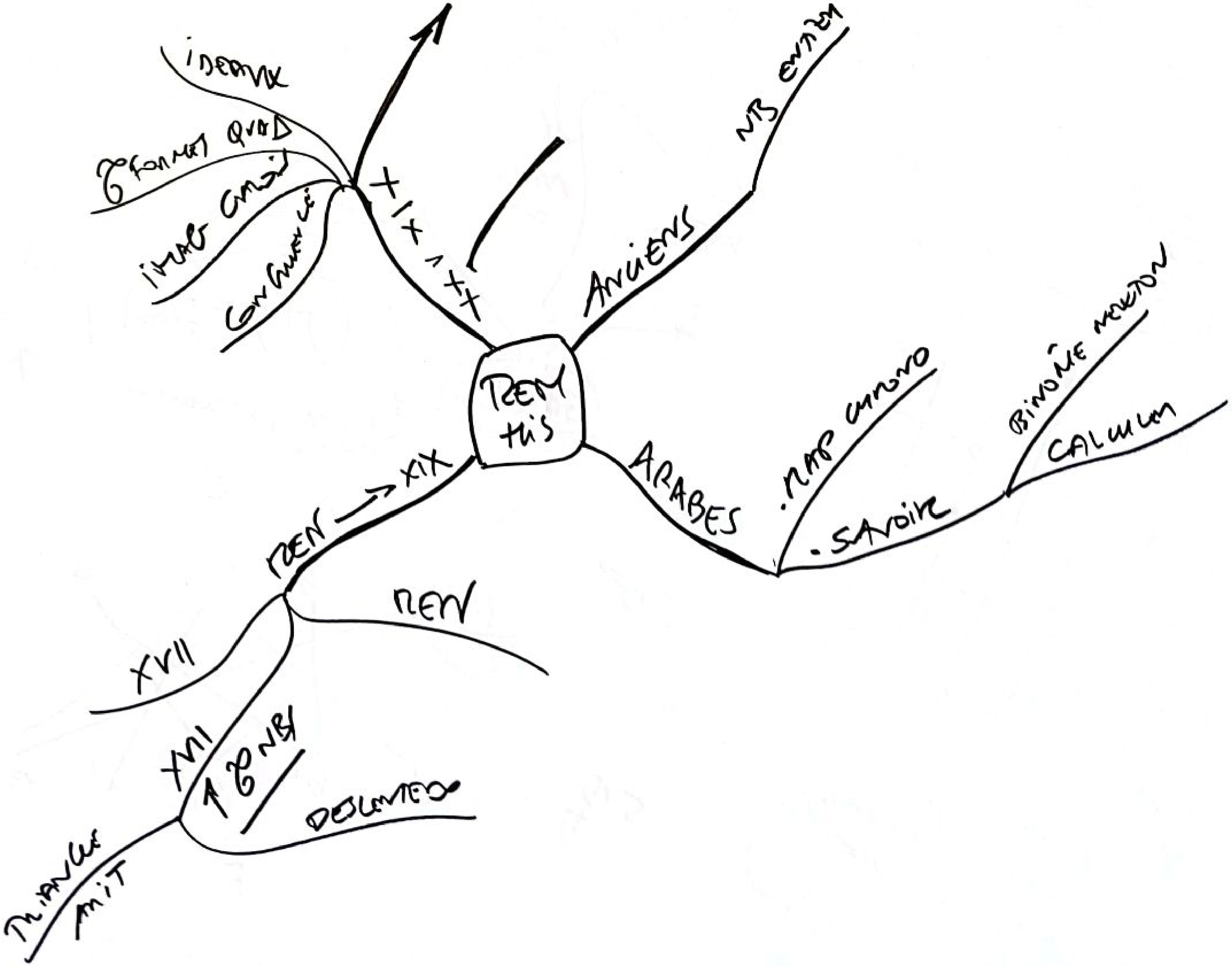


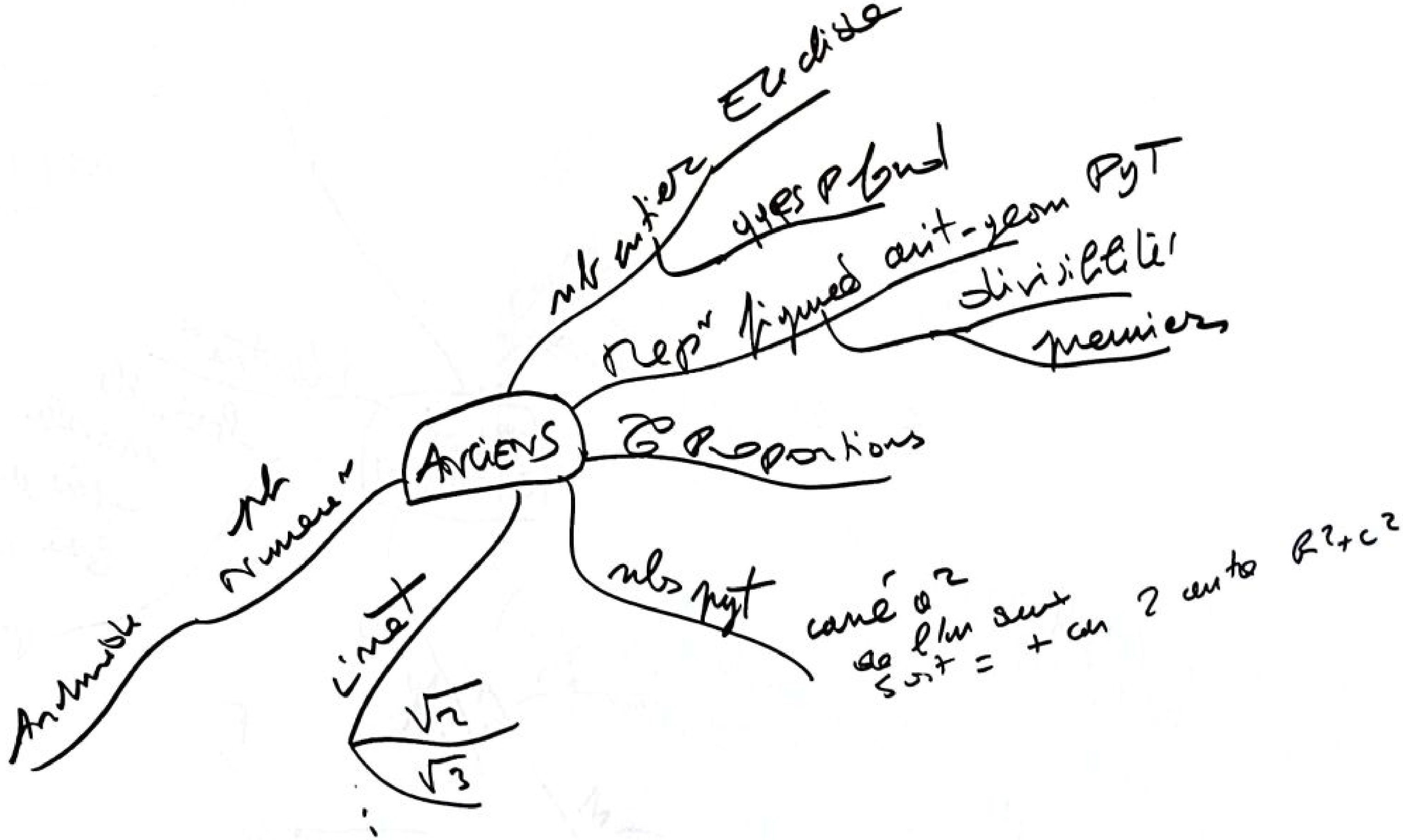
car col
ait & E nbs

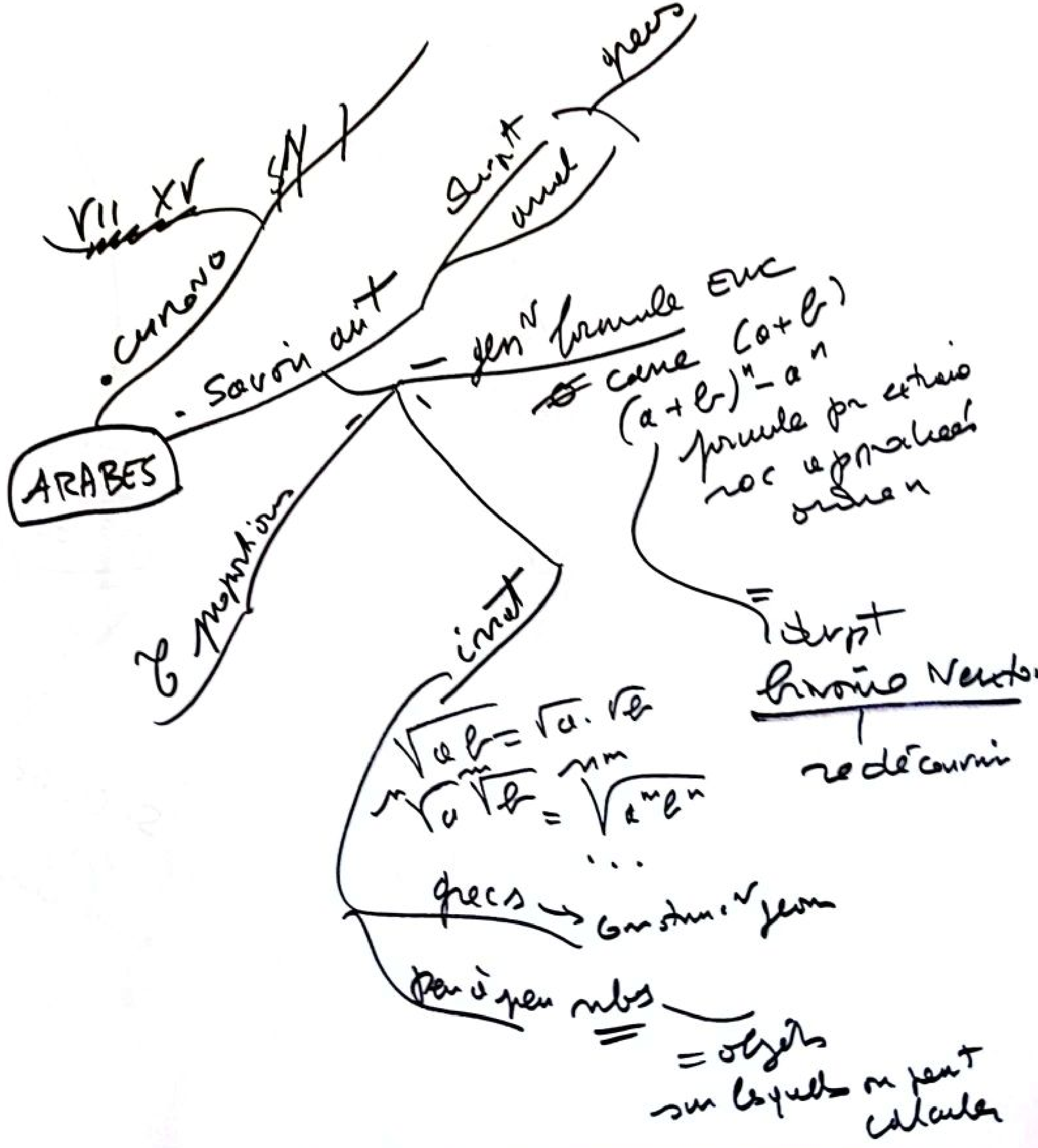
1

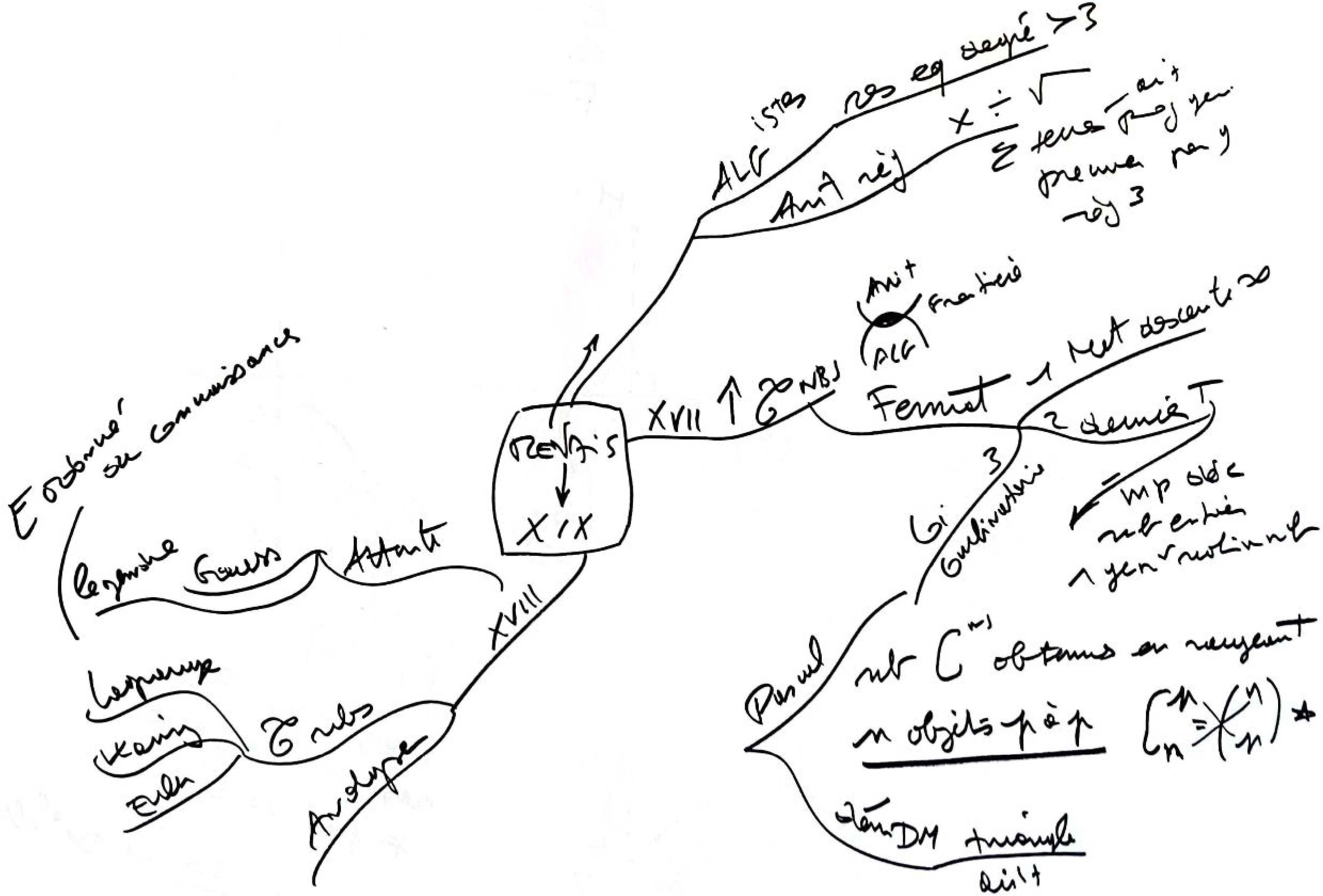
Cas cf
Rem historiques

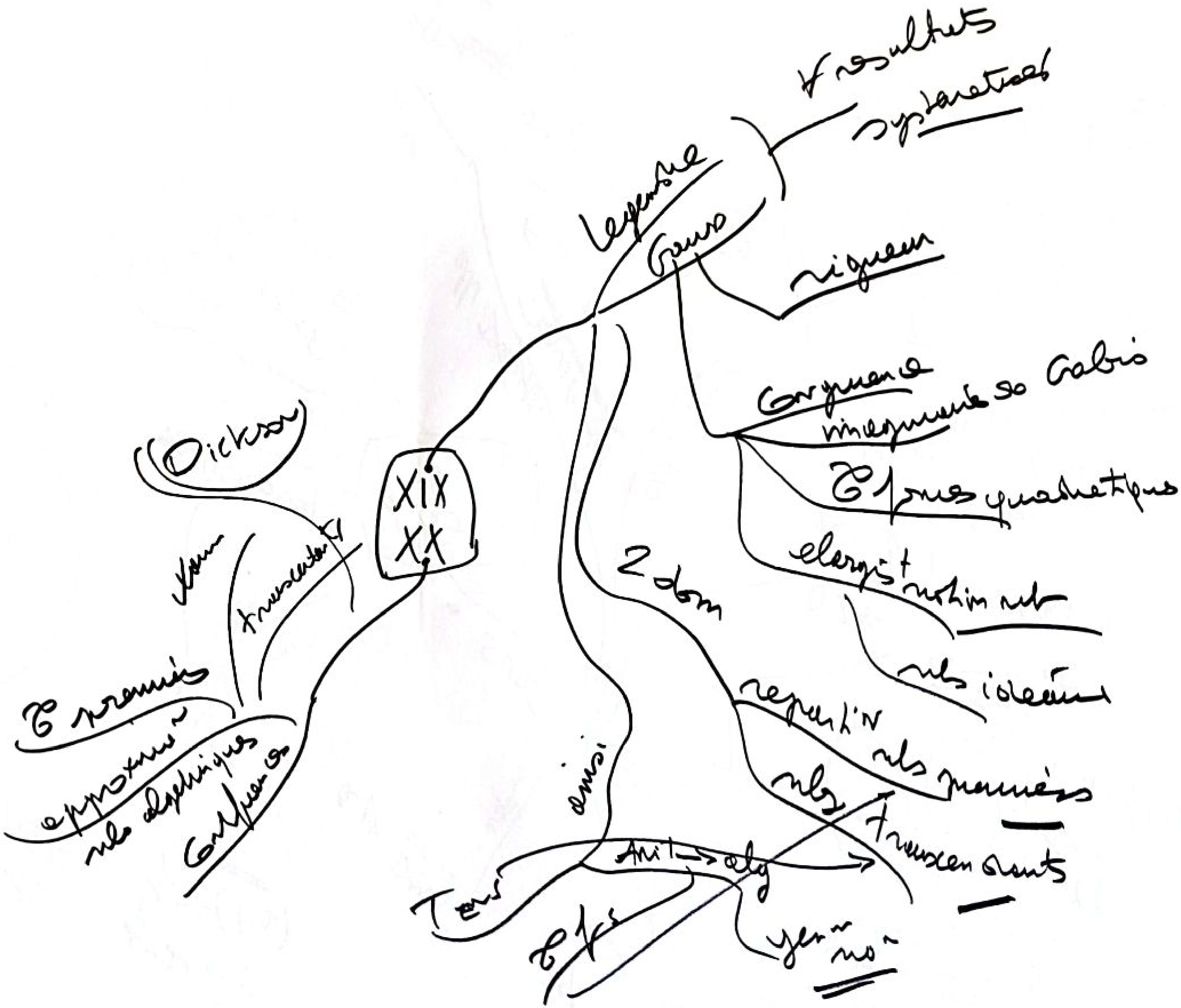


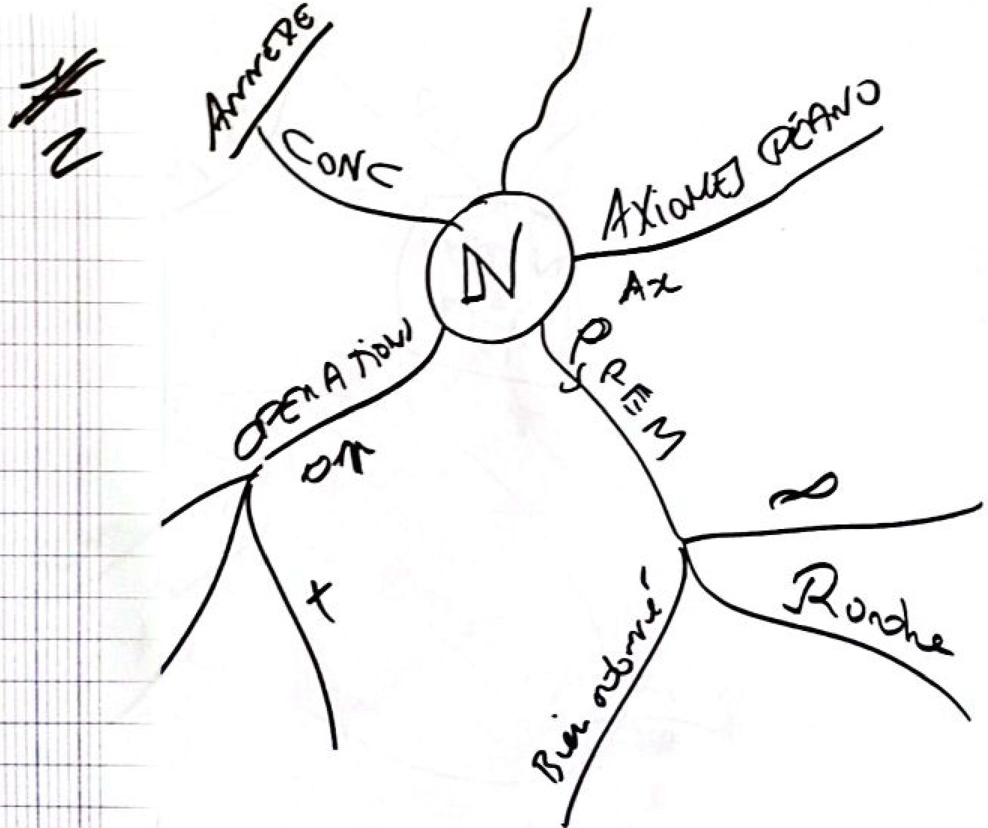

XIX → XX
ANCIENS
ARABES
. SAVOIR
BINÔME NEWTON
REN → XIX
REN
XVII
XVI


ANCIENS
Euclide
divisibilité
premiers
proportions
nbs pyt
√2
√3

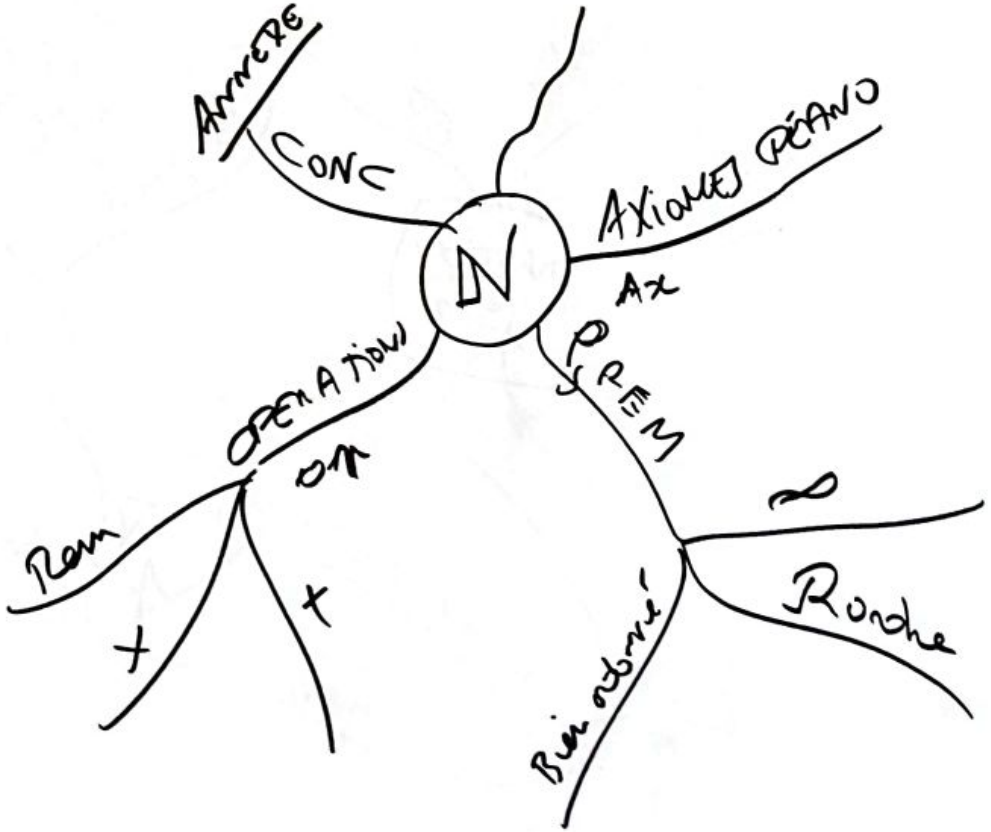

ARABES
• chrono
VII XV
• Savoir ant
surtout
grecs
— génⁿ formule Euc
carré (a+b)
(a+b)ⁿ − aⁿ
formule pr certains
nos approximations
ordre n
= interpt
binôme Newton
redécouvrir
proportions
irrat
√ab = √a · √b
ⁿ√a ᵐ√b = ⁿᵐ√(aᵐbⁿ)
...
grecs → construction géom
peu à peu nbs
= objets sur lesquels on peut calculer

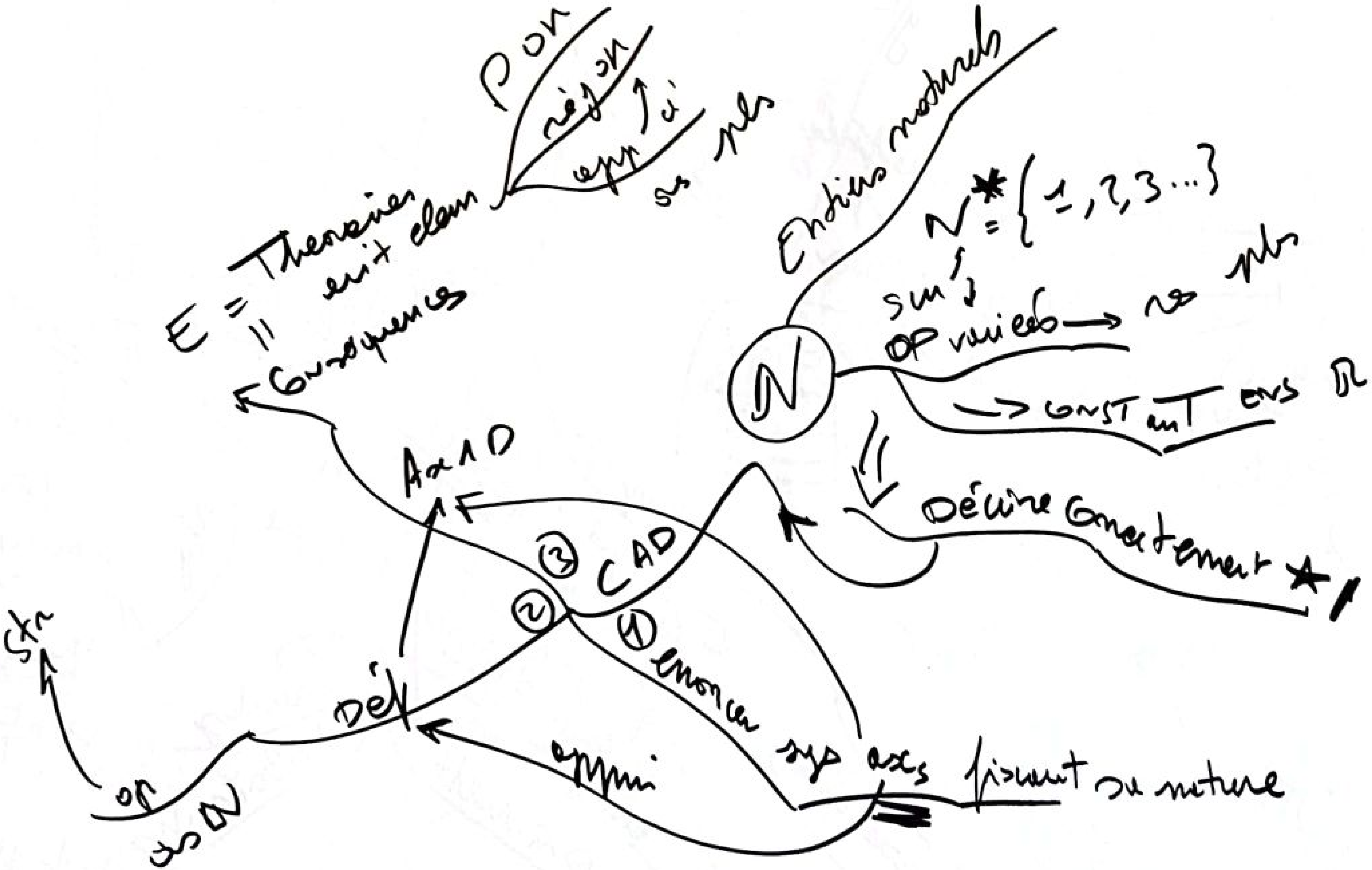

RENAIS
XIX
XVII
XVIII
ALG
res eq degré > 3
Arit nég
× ÷ √
Fermat
1 Met descente ∞
2 dernier T
3
Combinatoire
Loi
Pascal
nb C obtenus en rangeant
n objets p à p
Analyse
Legendre
Gauss
Lagrange
Euler

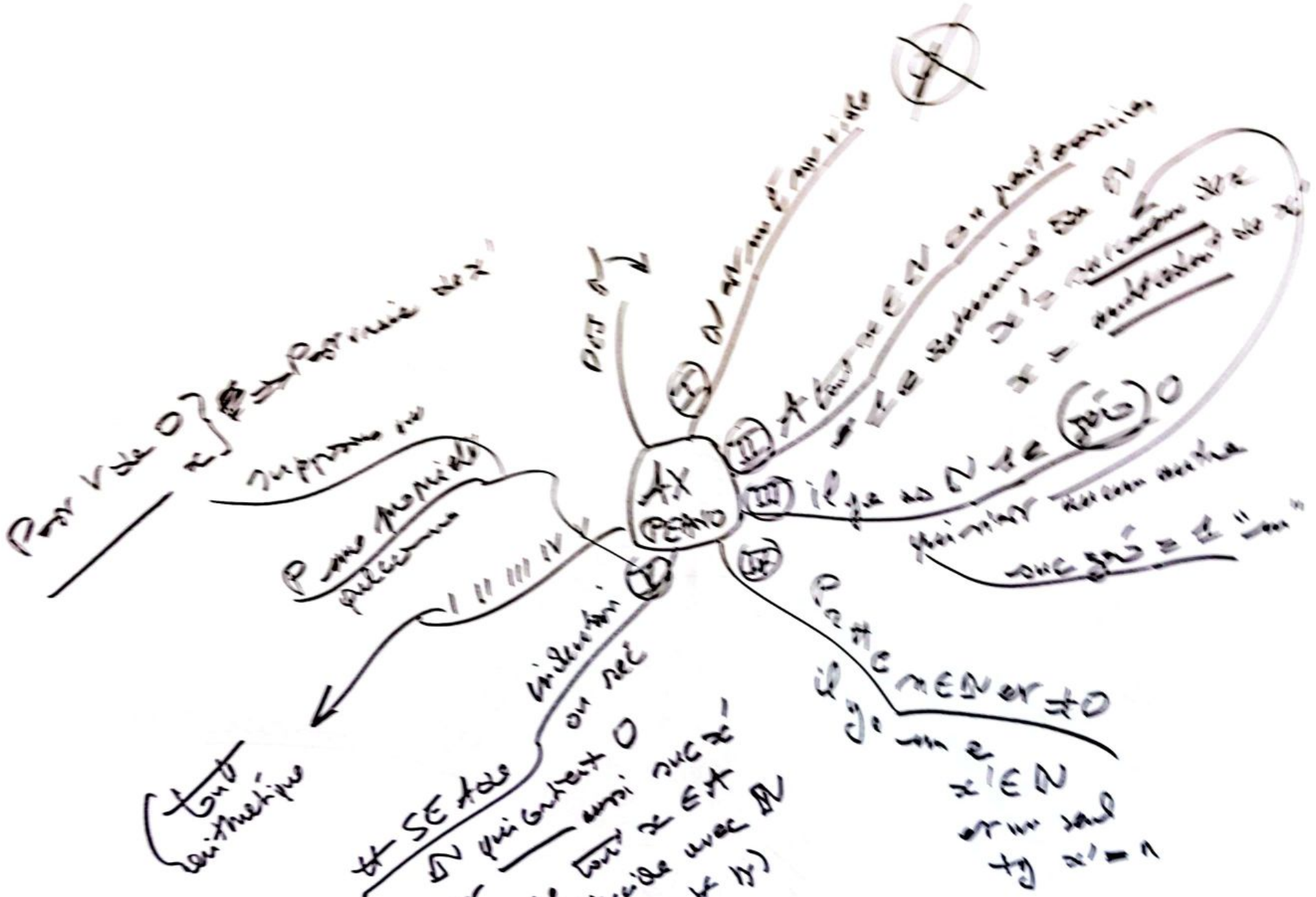

XIX
XX
Dickson
Legendre
Gauss
rigueur
2 dom
ainsi
Tour

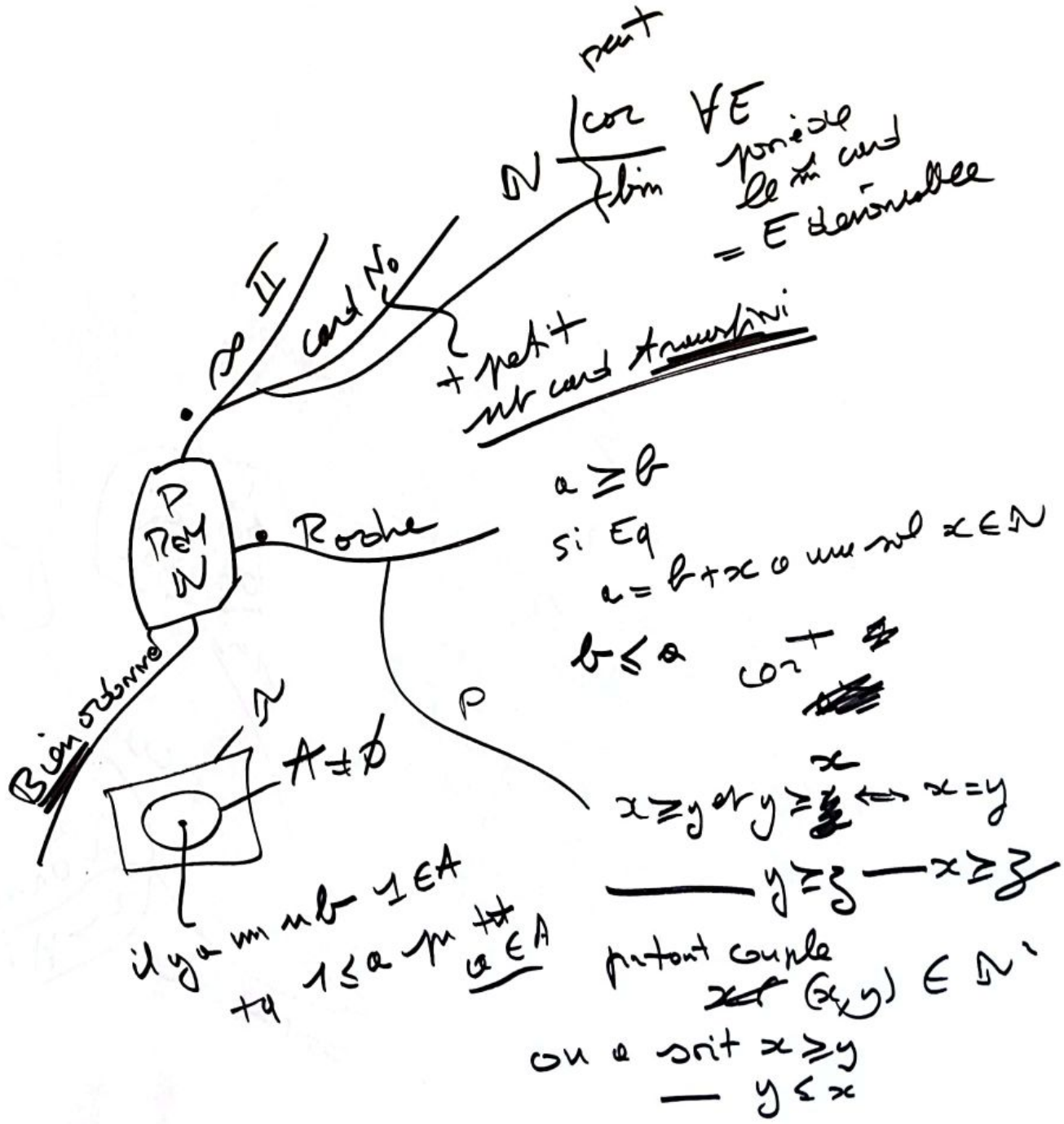


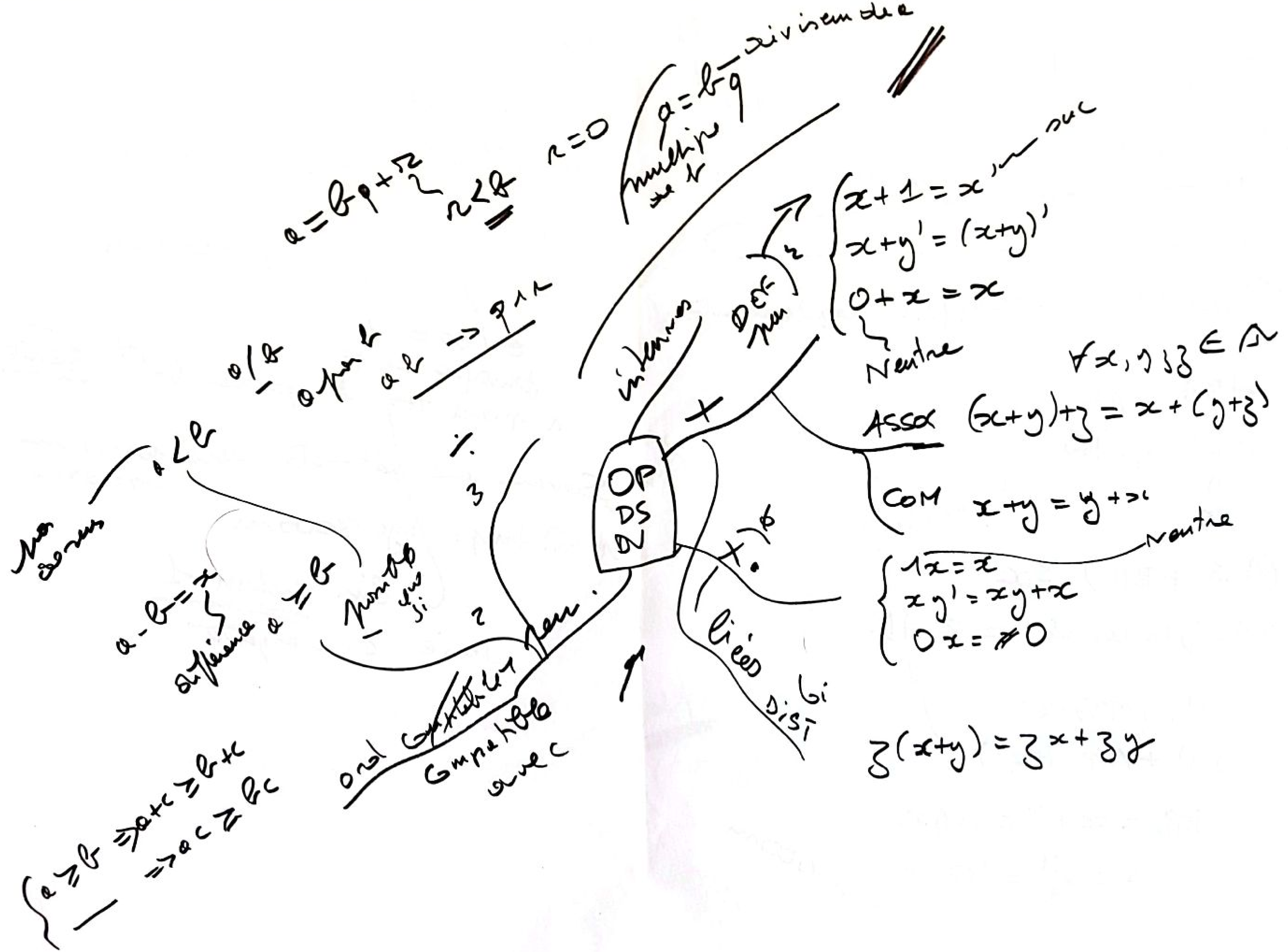
$\mathbb{N}$
CONC
AXIOMES PEANO
Ax
PREM
OPERATION
OP
+
Bien ordonné

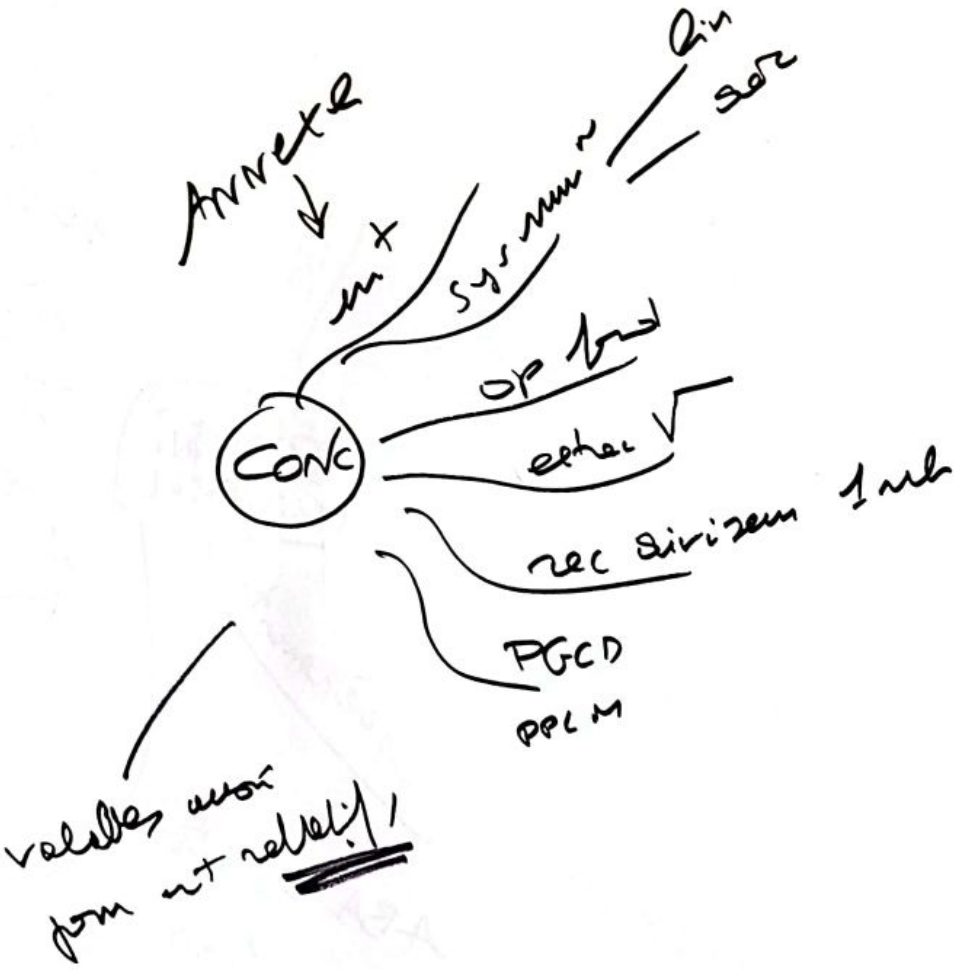

Arrivée
Conc
N
Axiomes Péano
Ax
Opérations
Opérations
Rem
x
+
Ordre
∞
Bien ordonné

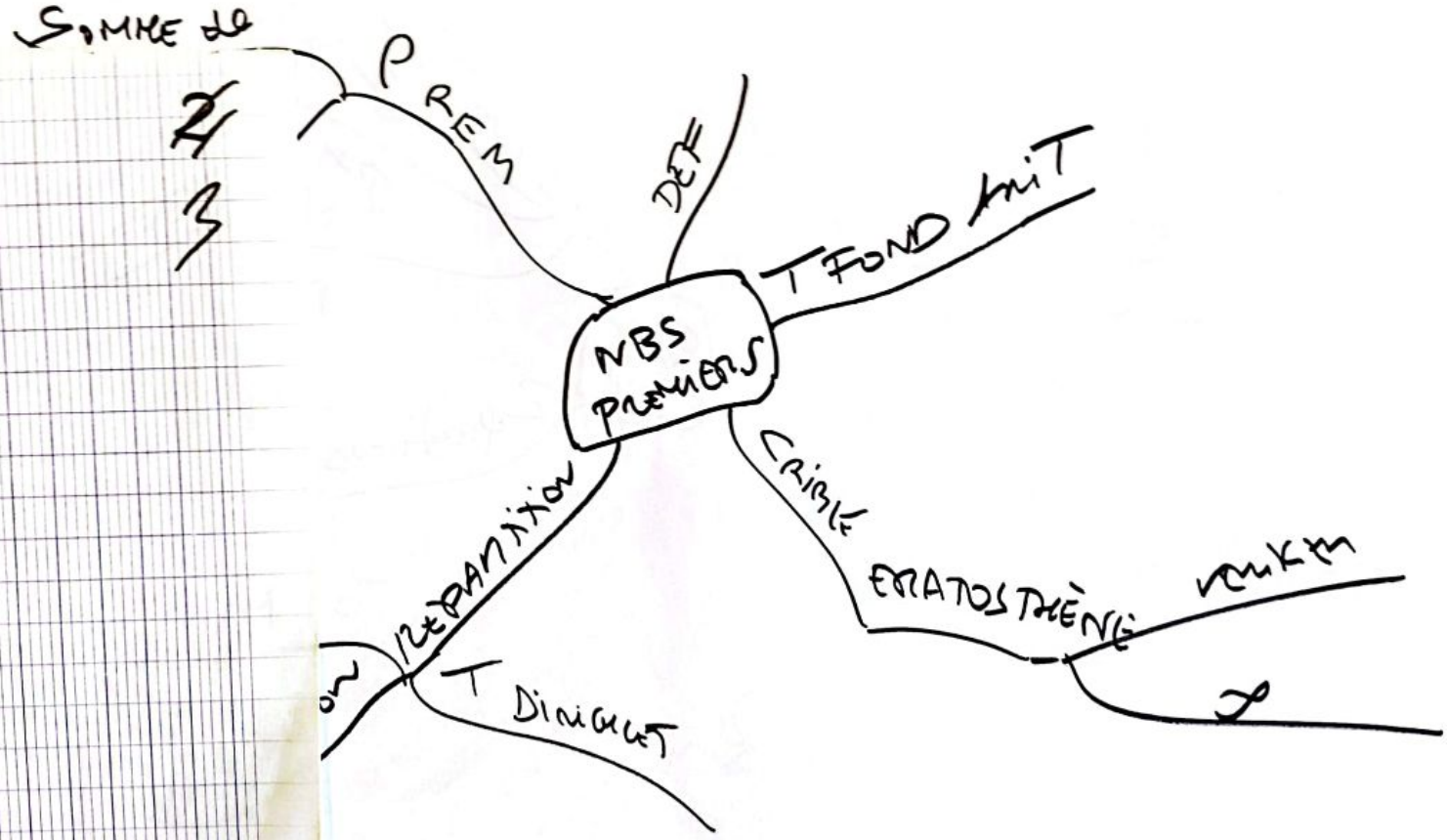

Entiers naturels
N* = {1, 2, 3 ...}
N
Décrire Exactement
CAD
Déf
Theoremes
Conséquences




peut
N
cor
lim
∀E
partie
de ℕ card
= E dénombrable
∞ ℕ
card ℕ₀
+ petit
ℕ card infini
P
Rel
ℕ
Rosbif
a ≥ b
si Eq
a = b + x a vec x ∈ ℕ
b ≤ a
Bien ordonné
ℕ
A ≠ ∅
il y a un nb 1 ∈ A
tq 1 ≤ a pr tt a ∈ A
P
x ≥ y or y ≥ x ⟺ x = y
— y ≥ y — x ≥ y
partout couple
(x,y) ∈ ℕ²
ou a soit x ≥ y
— y ≤ x

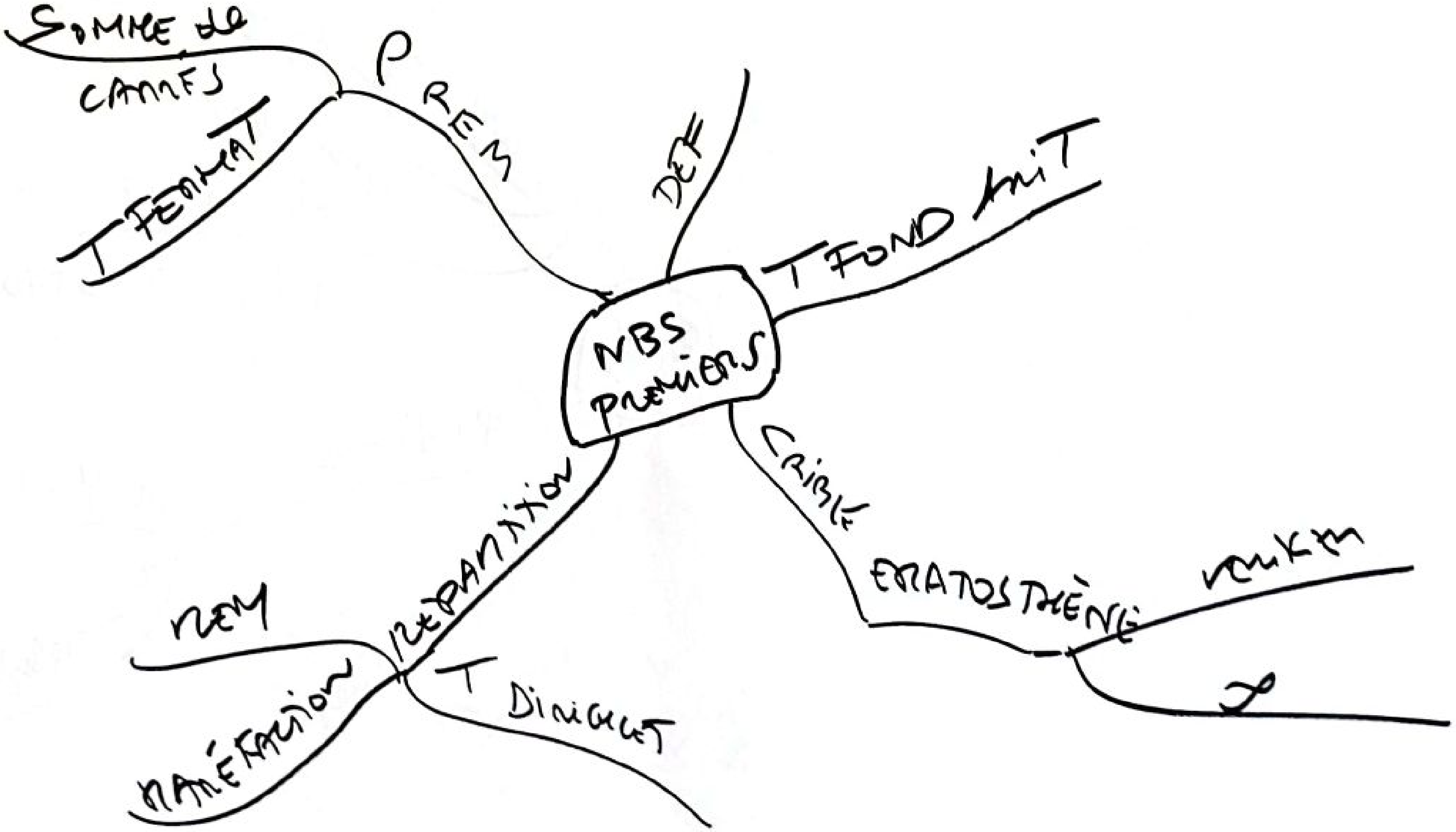

OP
DS
N
+
Déf par
x + 1 = x' succ
x + y' = (x + y)'
0 + x = x
Neutre
∀ x, y, z ∈ N
ASSOC (x + y) + z = x + (y + z)
COM x + y = y + x
×
1x = x
xy' = xy + x
0x = 0
neutre
liées
DIST
z(x + y) = zx + zy
internes
a = bq + r
r < b
r = 0
a = bq
multiple de b
diviseur de a
a/b
a par b
a b → q r
%
3
2
−
a < b
non sens
a − b = x
différence a ≥ b
possible ssi
ordre
compatible avec
a ≥ b ⇒ a + c ≥ b + c
⇒ ac ≥ bc

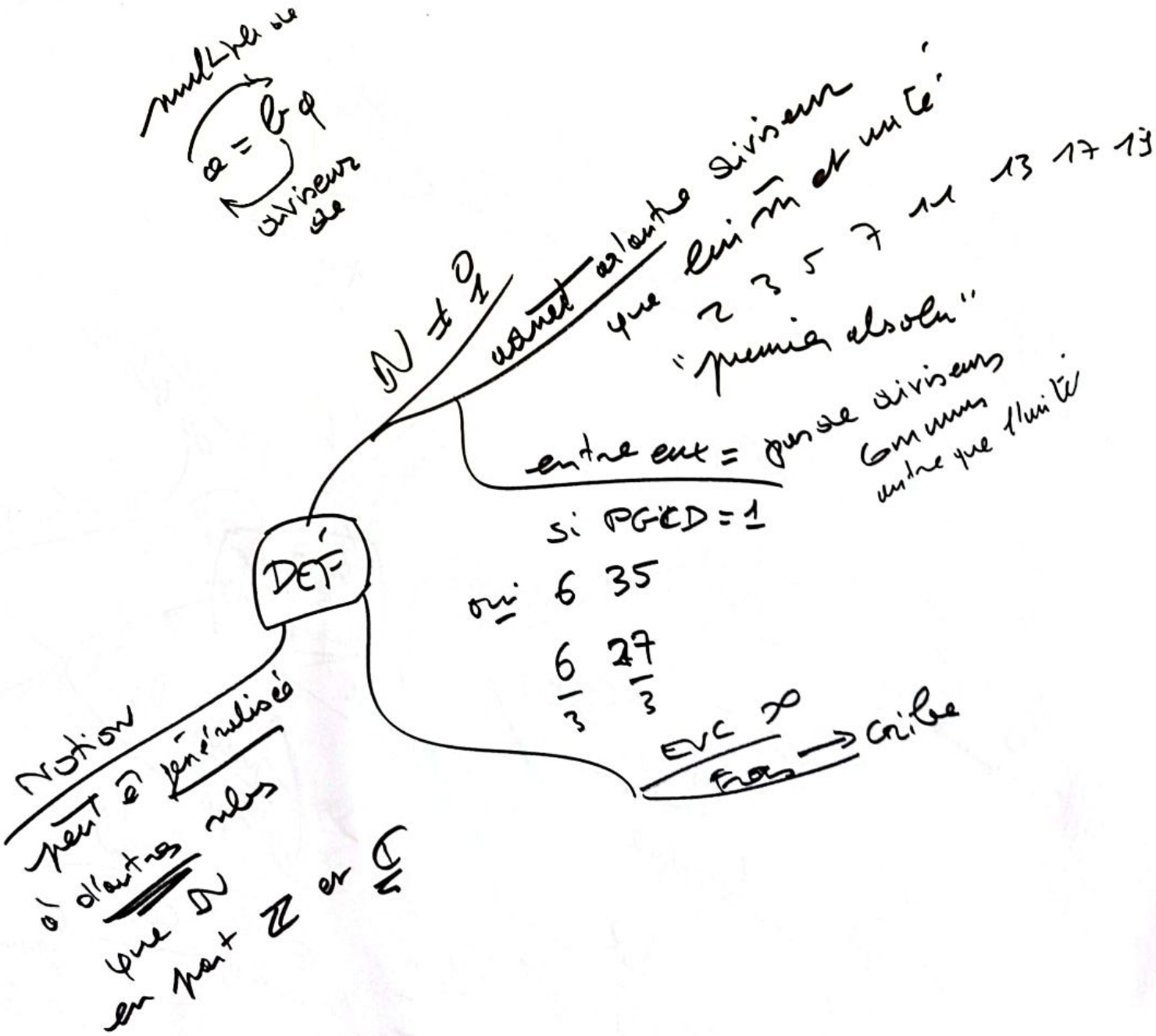

Annexe
CONC
PGCD
PPCM



Ca col

nbs premiers


NBS PREMIERS
PREM
SOMME DE CARRÉS
T FERMAT
DEF
T FOND ARIT
CRIBLE
ERATOSTHÈNE
∞
RÉPARTITION
REM
T DIRICHLET


multiple de
a = b q
diviseur de
N ≠ 0 1
admet comme diviseurs
que lui-même et un
2 3 5 7 11 13 17 19
"premier absolu"
entre eux = pas de diviseurs communs autre que l'unité
si PGCD = 1
ou 6 35
6/3 27/3
DET
Notion
peut se généraliser
à d'autres ensembles
que N
en plus Z et D
EVC ∞
Finis → cribe

$a = 6600$

$\frac{6600}{2} \Rightarrow q_1 = 3300$

$\frac{3300}{2} \Rightarrow r_2 = 1650$

$\frac{1650}{2} \Rightarrow q_3 = 825$

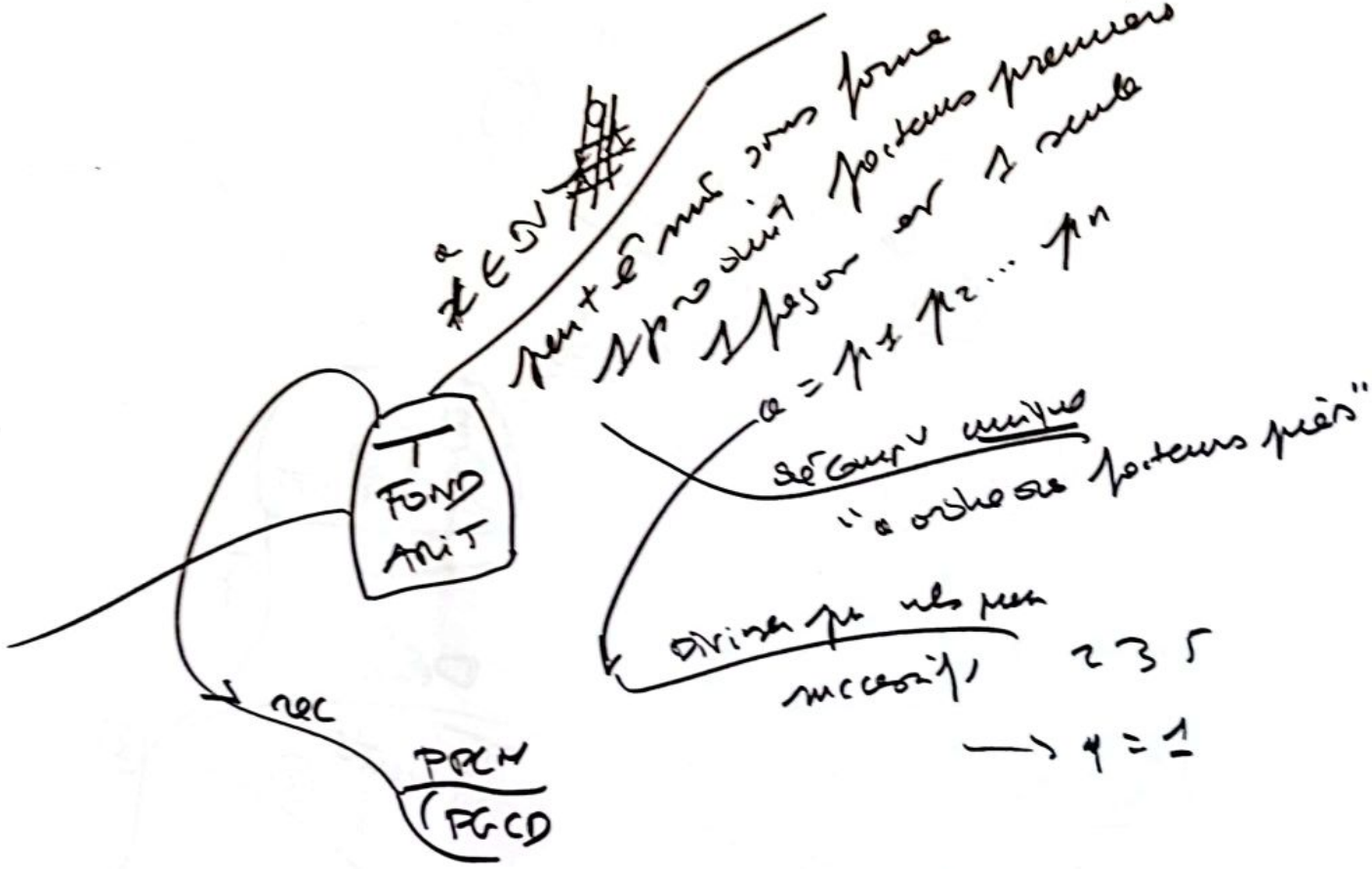
$\frac{825}{3} = q_4 = 275$

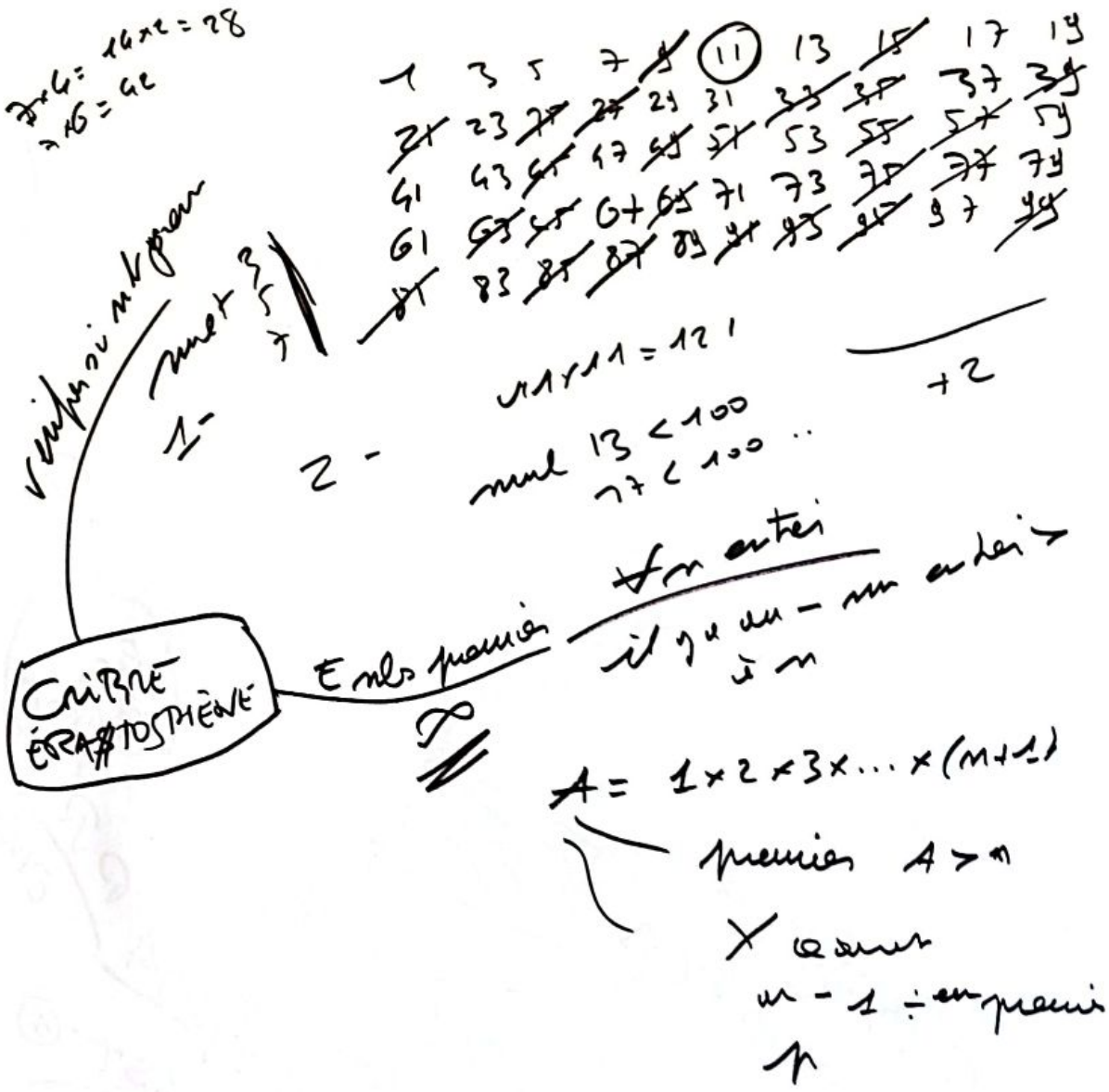
$q_5 = 55 \quad q_6 = \frac{11}{=} q_{min}$

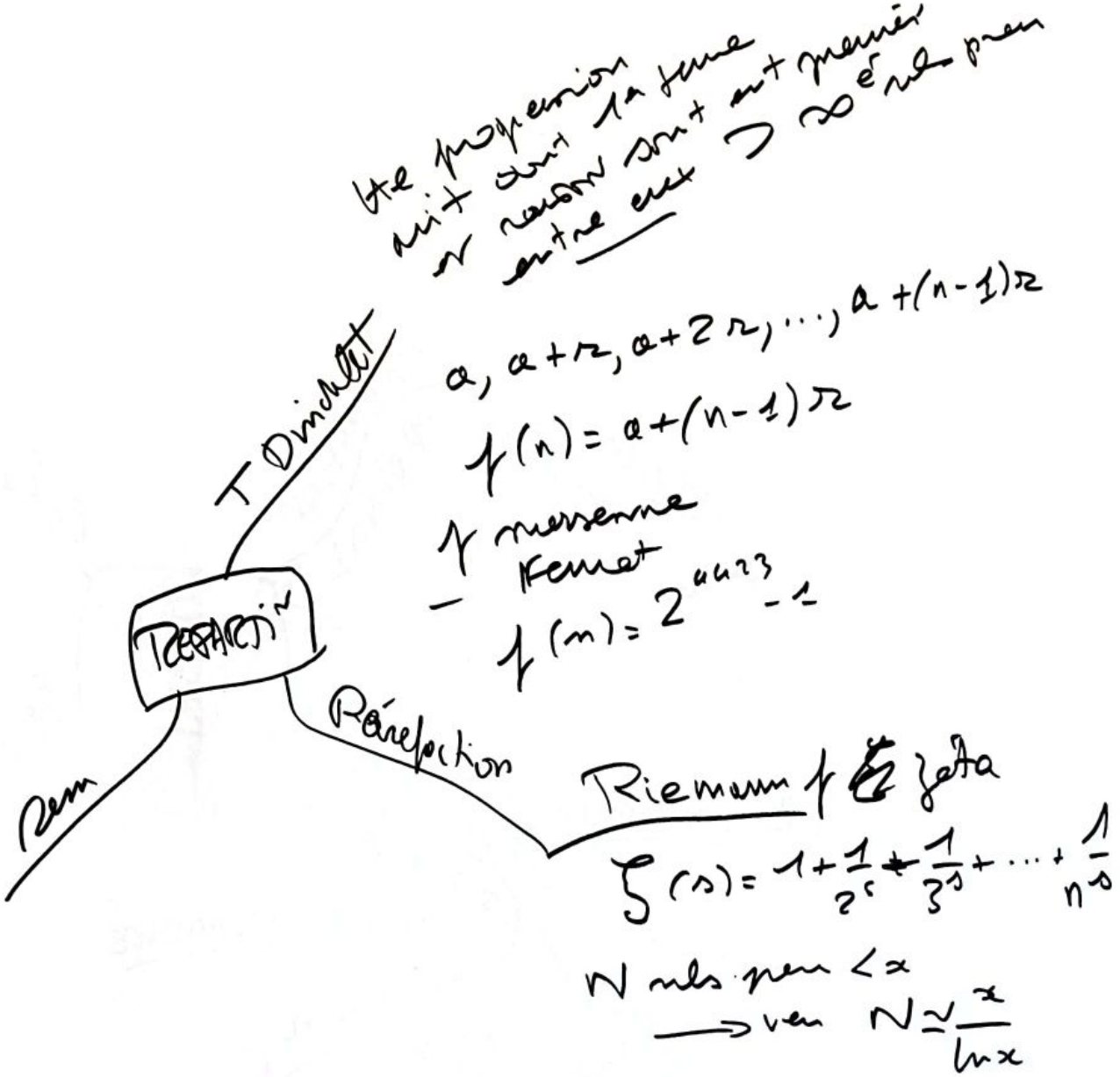
6600	2
3300	2
1650	2
825	3
275	5
55	5
11	11
1	

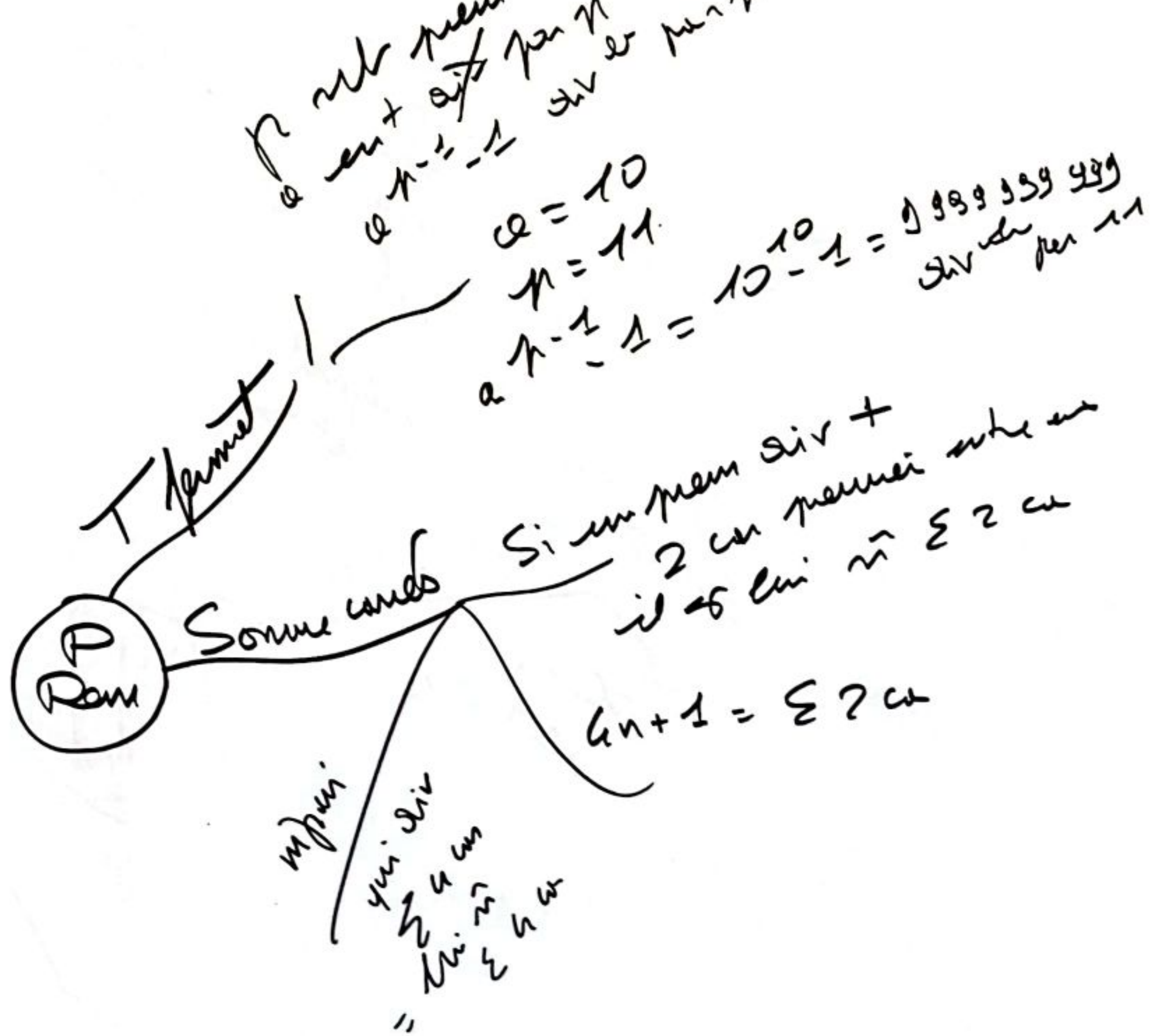
$= 2 \times 2 \times 2 \times 3 \times 5 \times 5 \times 11$

$= 2^3 \times 3 \times 5^2 \times 11$

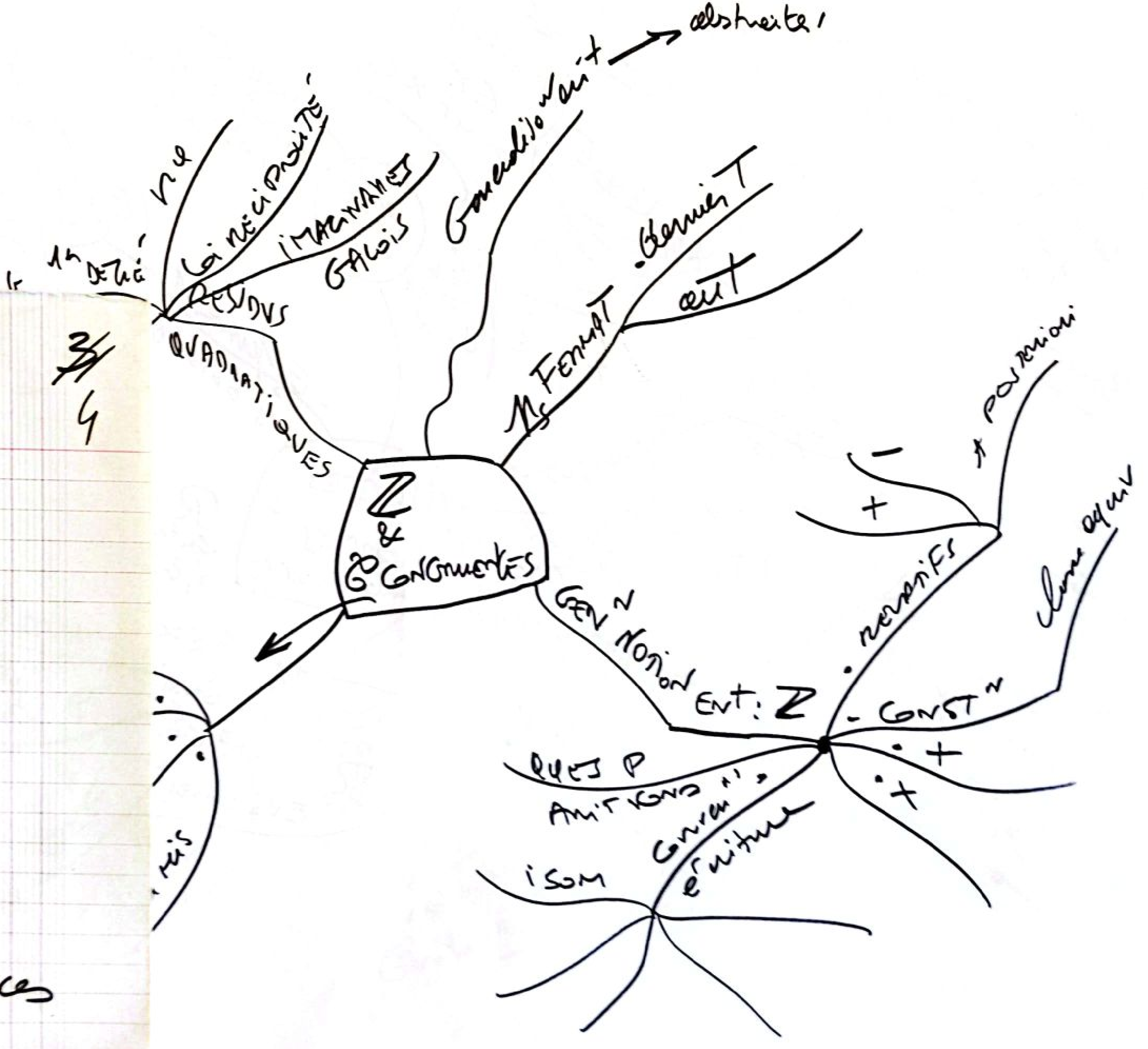



CRIBLE ÉRATOSTHÈNE
1-
2-
+2
∞

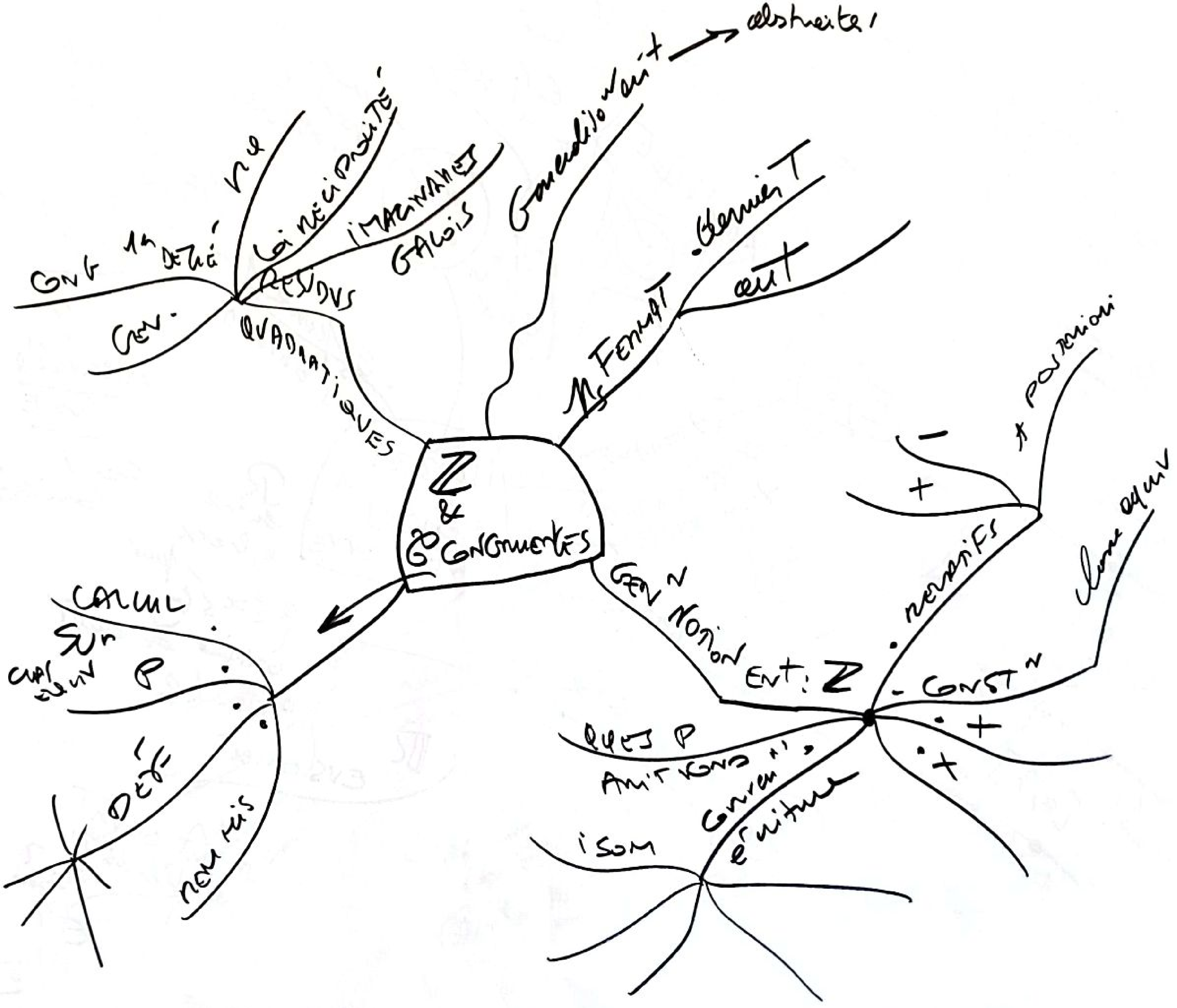

Ste progression arit dont 1a forme or nombres sont ent premiers entre eux ⇒ ∞ nbs prem
T Dirichlet
a, a+r, a+2r, ..., a+(n-1)r
f(n) = a+(n-1)r
f mersenne
- Fermat
f(n) = 2^aur3 - 1
TCFARITH
Rém
Réciprocité
Riemann f ζ zeta
ζ(s) = 1 + 1/2^s + 1/3^s + ... + 1/n^s
N nbs prem < x
→ ven N ≃ x/ln x


P Prem
T Fermat
p nbr prem
a ent div par p
a^{p-1} - 1 div par p
a = 10
p = 11
a^{p-1} - 1 = 10^{10} - 1 = 9 999 999 999 divisible par 11
Somme carrés
Si un prem div + 2 car premiers entre eux il est lui-même Σ 2 ca
4n + 1 = Σ 2 ca

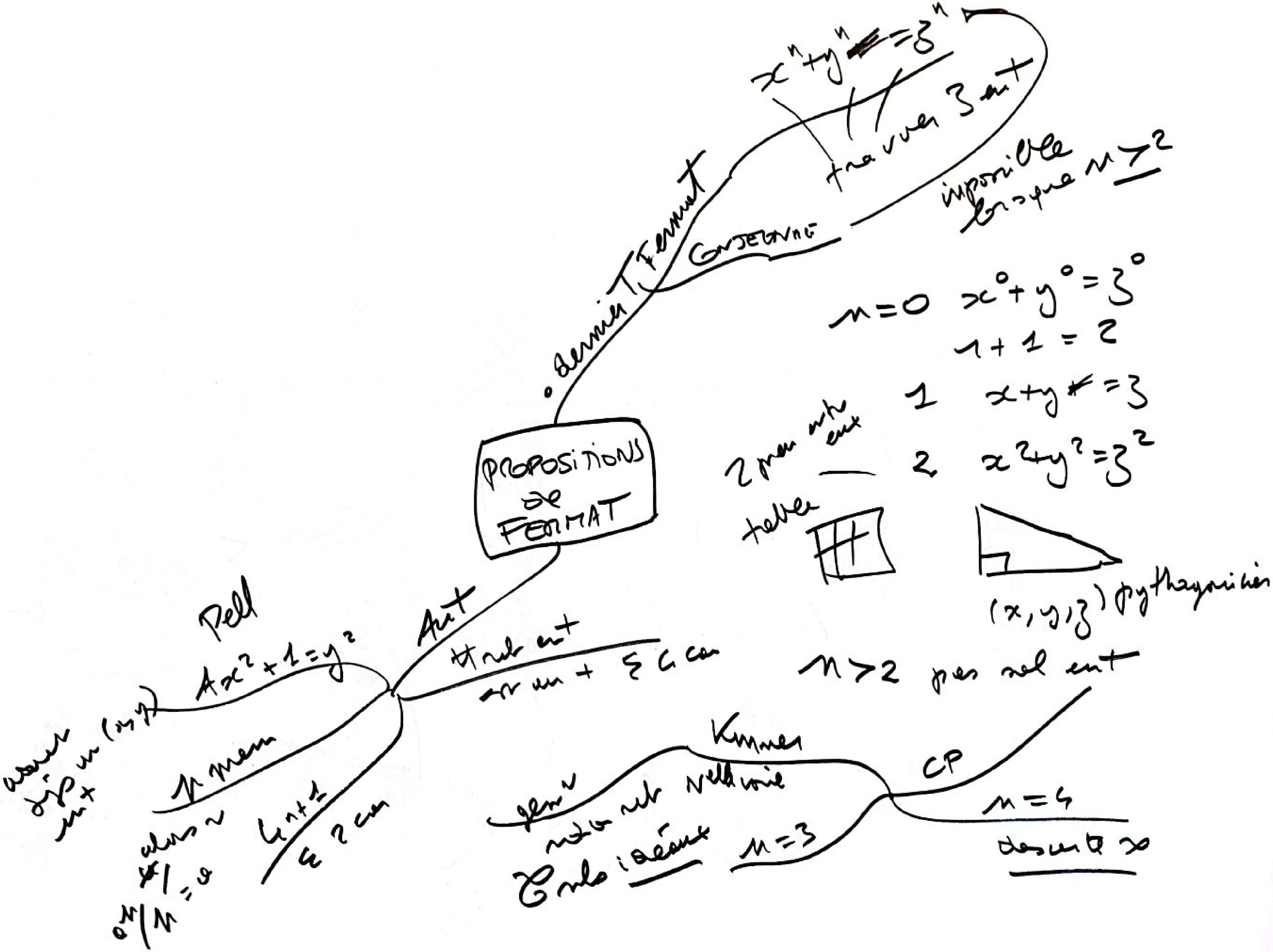
4



Cal vol
Z & C Congruences



Z
&
congruences
Quadratiques
Résidus
Gén.
Cong 1er degré
Réciprocité
Imaginaires
Galois
Fermat
Calcul
Déf
Gén° notion
Ent.: Z
Const°
+
×
−
+
Négatifs
Isom



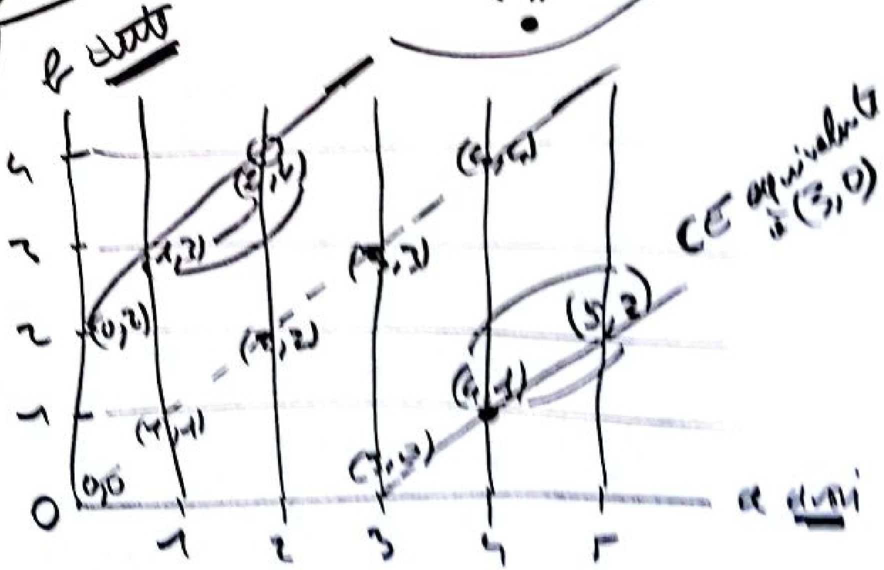
PROPOSITIONS DE FERMAT
$x^n+y^n=z^n$
$n=0$ $x^0+y^0=z^0$
$1+1=2$
$x+y=z$
$x^2+y^2=z^2$
(x,y,z) pythagoriciens
$n>2$ pas sol ent
CP
$n=4$
Kummer
$n=3$
Pell
$Ax^2+1=y^2$

Const^n de $\mathbb{Z}$

- relatifs
  - 0
  - +
  - −
  - hist^t : nombres neg $x + 1 = 0$
    - reçus XV/XVI siècle
    - a posteriori
      - + abstraits
      - + gén
      - ↳ Comprendre

- +
  - $x = \overline{(a,b)}$
  - $y = \overline{(c,d)}$
  - $\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c,\ b+d)}$ (ds $\mathbb{Z}$ / ds $\mathbb{N}$)
  - 1. $\overline{(0,0)}$ N
    - $\overline{(a,b)} + \overline{(0,0)} = \overline{(a,b)}$
    - + $\overline{0}$
    - $= 0_{\mathbb{Z}}$
  - 2. C + A
  - 3. $\overline{(a,b)} + \overline{(b,a)} = \overline{(a+b,\ a+b)}$ opposés

- Construc^n
  - $\mathbb{N} \times \mathbb{N}$
  - (a,b)
  - (a,b) • $(0,2)$



- • $b < a$
- ○ $a < b$
- $(4,1) \mathcal{E} (5,2)$
- $4 + 2 = 5 + 1 = 6$

- Déf
  - R équiv $\mathcal{E}$
  - $(a,b)\ \mathcal{E}\ (a',b')$
  - ⇕
  - $\mathcal{E} : a + b' = b + a'$
  - + 2 couples (a',b')
  - + q équi à (a,b) selon $\mathcal{E}$

- $\mathbb{Z}$ = ens CE ~~disjointe~~ Bourbaking

- ens relatifs particuliers

NB: trouver une CE $\overline{(a,b)} = x$

Gén Notion NB $\mathbb{Z}$

SYM × +0 opposé
inverse

×

$\overline{(a,b)} \times \overline{(c,d)} = \overline{(ac+bd,\ ad+bc)}$

C
A
D/+

$\overline{(1,0)}$ N
$\overline{(a,b)} \times \overline{(1,0)}$
$\times \overline{(a,b)} = \overline{(a,b)} \times \overline{(1,0)}$
$= \overline{(a+0,\ 0+b)} = \overline{(a,b)}$

Correspon
écriture

1 $\overline{(a,b)}$ repr par (m, 0) ou (0, m)
de la classe
∃ ou 0

$= \{ (4,0), (5,1) \}$

$\overline{C,0}$ (0, 2)

2
$(m, 0) = +m$
$(0, m) = -m$
$(0, 0) = 0$
celui CE
écrite
canonique

relatif écrit
par m valeur absolue ou (m, 0)
1 par un signe + ou −

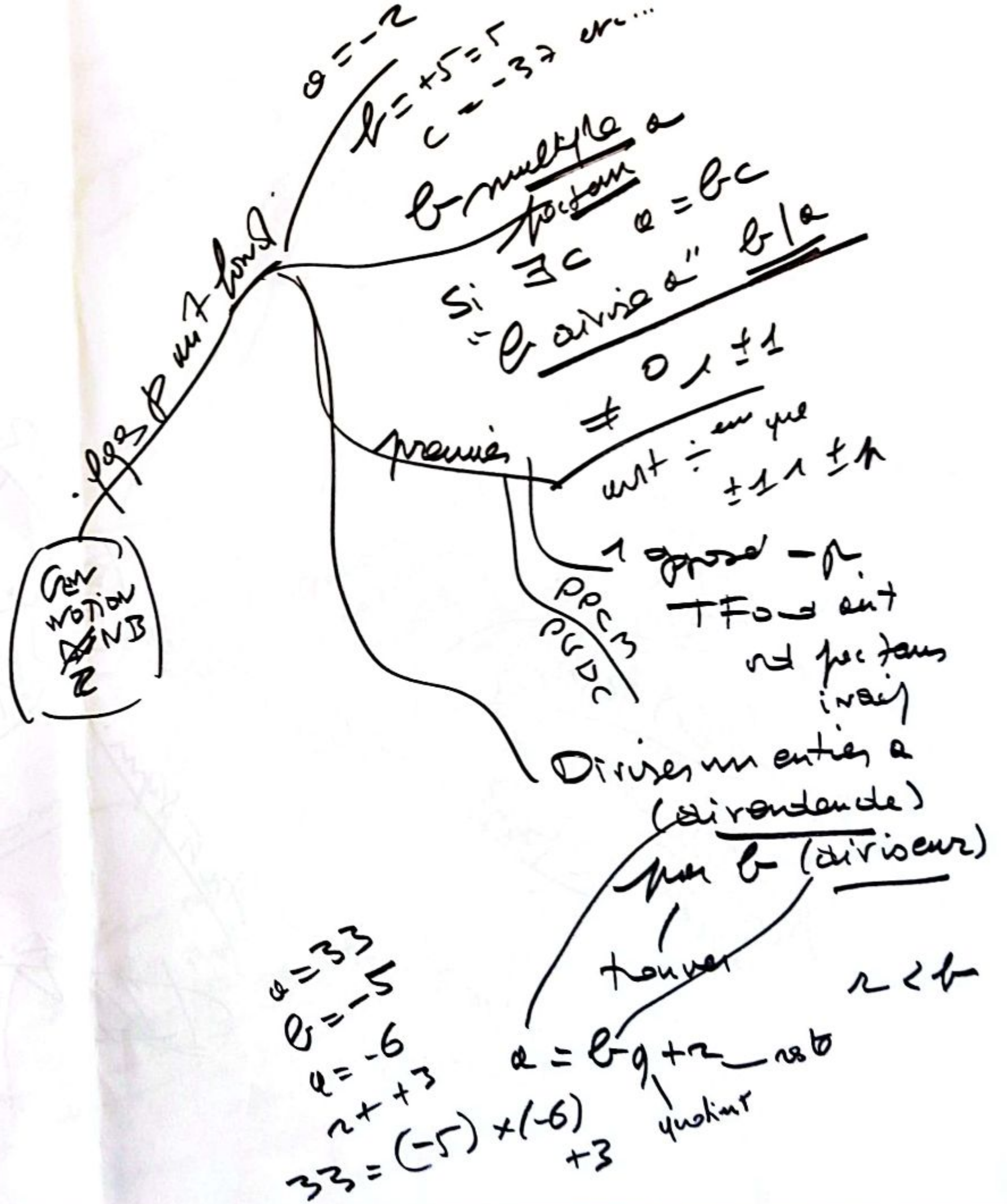
3
$(\mathbb{Z}, \leq)$
ttout − < 0 < ttout +
de signe
le pt celui
a la + pt VA
∃ min
max

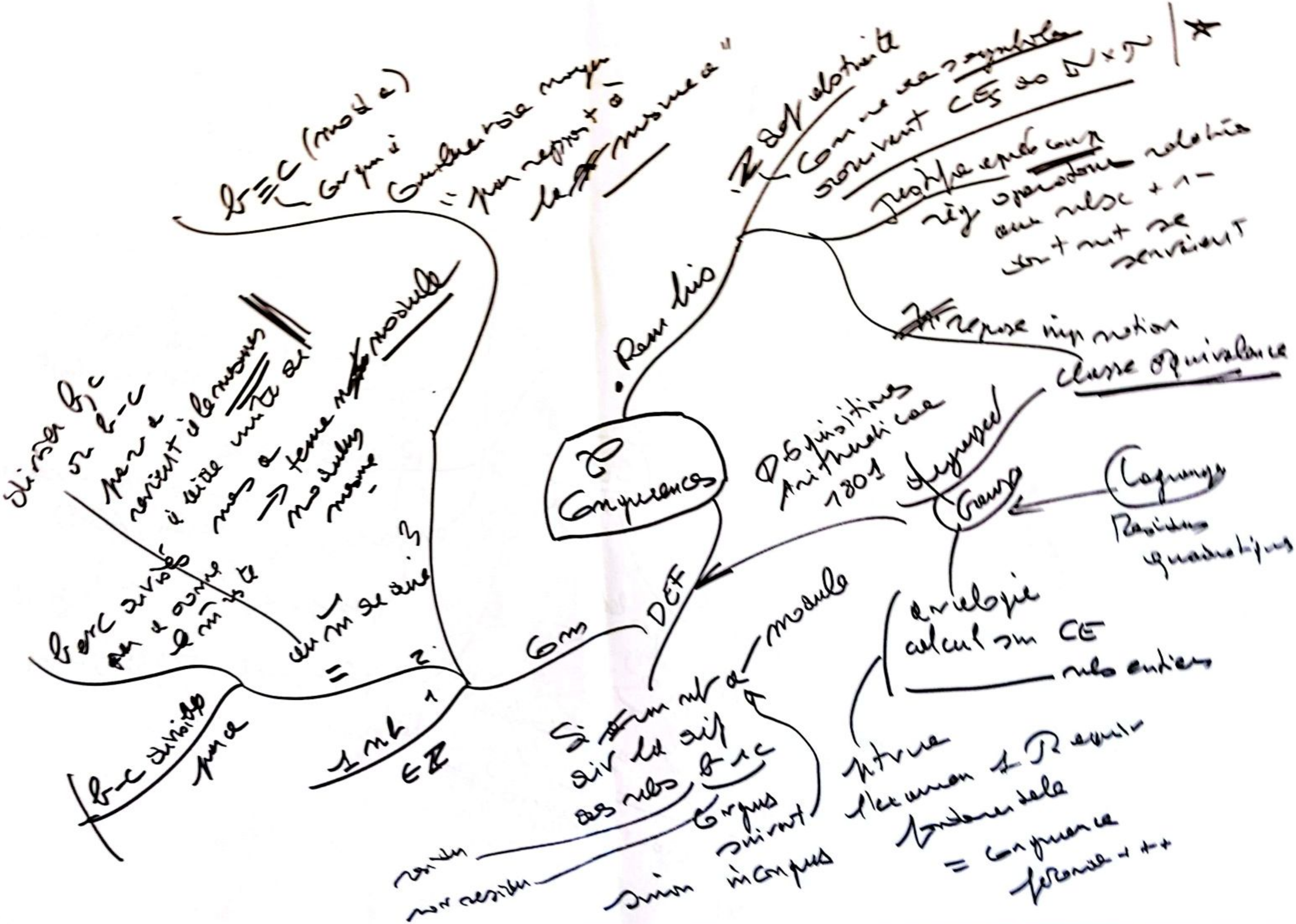
4
règ simpli
simples
justifier par calc
+ 1 ×

ANNEXE
$\mathbb{Z}$
calculs

$|-2| = 2 < |4| = 4$
$-2 > -4$
$+2 < +4$

5
isotom
$\mathbb{N}^+$ $\mathbb{Z}^+$
peut identifier
ces 2 en
1 identif tm avec m


a = -2
b = +5 = 5
c = -3
etc...
b multiple a
facteur
Si ∃c a = bc
« b divise a » b|a
0, ±1
≠
premier
±1, ±n
PPCM
PGCD
Diviser un entier a
(dividende)
par b (diviseur)
trouver
a = bq + r
reste
quotient
r < b
a = 33
b = -5
q = -6
r = +3
33 = (-5) × (-6) + 3


Congruences
DEF
Rem hist
Disquisitiones Arithmeticae
1801
Gauss
Lagrange
Résidus quadratiques
classe équivalence
module
analogie
calcul sur CE
nbs entiers
∈ Z

Cong

Com

(3)

$b \equiv c \pmod a$

résidu de b / modulo a

Congruence elle même traduit le fait que $b - c$ est divisible par a

Mais si $b - c$ divisible par a, $c - b$ aussi

$c \equiv b \pmod a$

résidu de c / modulo a

(4) Ex

$22 \equiv 7 \pmod 5$

$22 - 7$ divisible par 5

22 et 7 divisés par 5 donnent même reste ici 2

$22 \equiv x \pmod 5$

$x = 2$
$x = 12$
$x = 17$

val de x qui satisfont à cong sont les racines de la cong considérée

$x \equiv 0 \pmod 2$

$x - 0$ divisible par 2

$= x$ entier pair

impair $y \equiv 1 \pmod 2$

(5)

$a \equiv r \pmod p$

reste de la ÷ de a par p

Relié à D ÷ Z

Cong 6

notée symboliquement R ÷ e

peut traduire la cong

÷ par

$a - r = pq$

0, 1, n

$a = pq + r$

$r < p$

$x/2 = \overline{0}$

$x = \overline{0}$

x sor un $\overline{0}$

$\overline{1}$

donc nb pairs

$y \equiv 1 \pmod 2$

$x \equiv 0 \pmod 2$

EX

CE de $\mathbb{Z}$

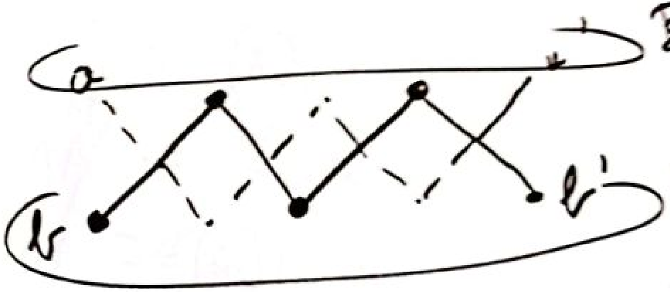
ts ent x qui vérifient une cong déterminée forment une

$\mathbb{Z}$

GNC

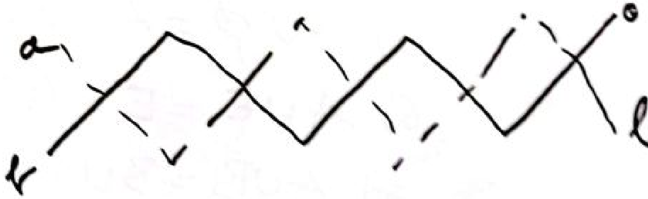
notion symb + R divisibilité

Pb tisserand



rubans circulaires

~~Couture~~ conjointe



Couture opposants

tâtonnements

~~Couture~~ si nb croisements pair

C = nb croisements
$\equiv 0 \pmod 2$

opposants ... un nb simple
1 + ...
nb x plus croisements ont

Généralités $P_{n+1}x$

PS

Requiv de $\mathbb{Z}$

R
S
T
(mod n)

$a \equiv a \pmod n$

$a \equiv b \pmod n \iff b \equiv a$

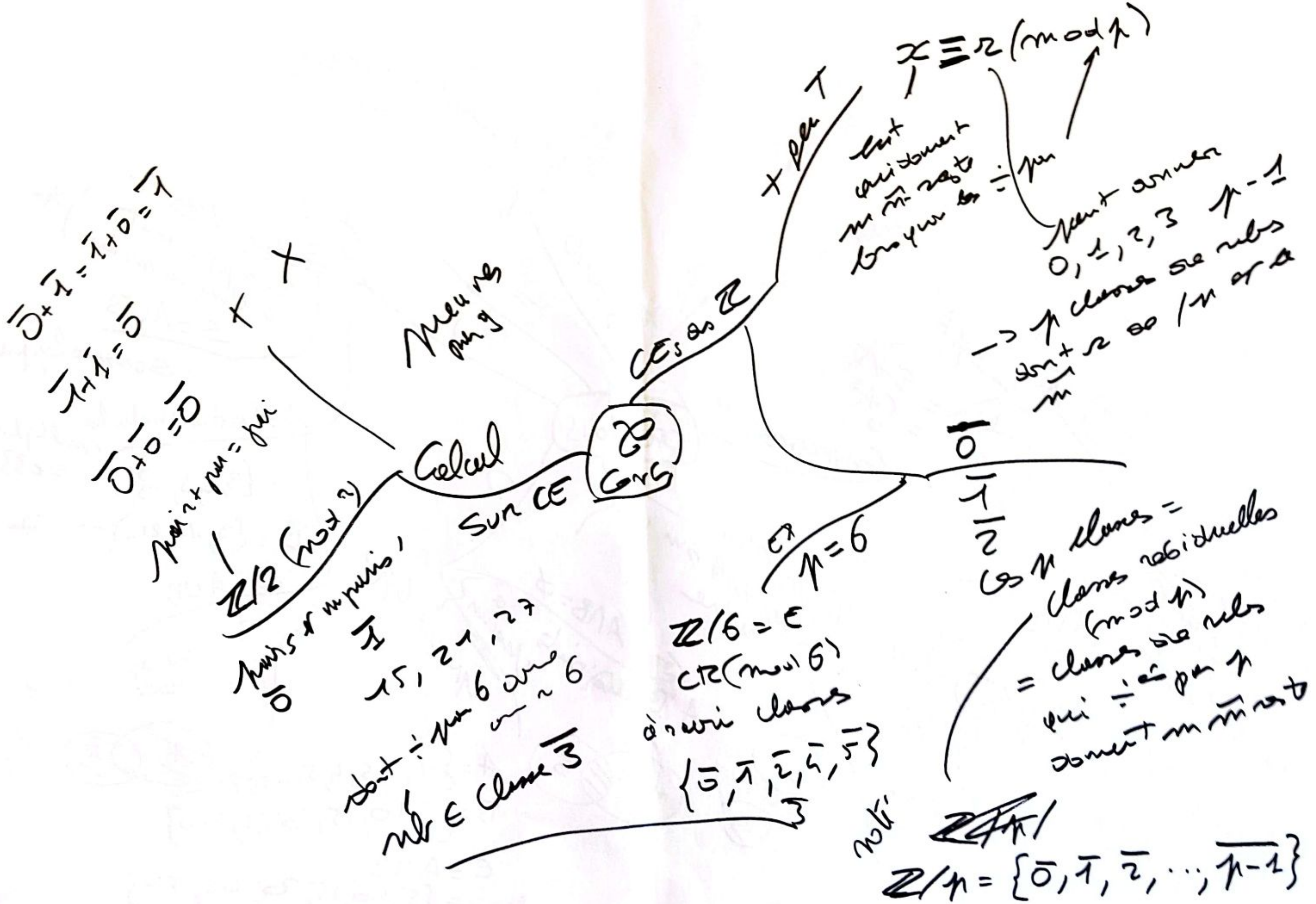
$a \equiv b \wedge b \equiv c \iff a \equiv c$

$a \equiv b \pmod n$

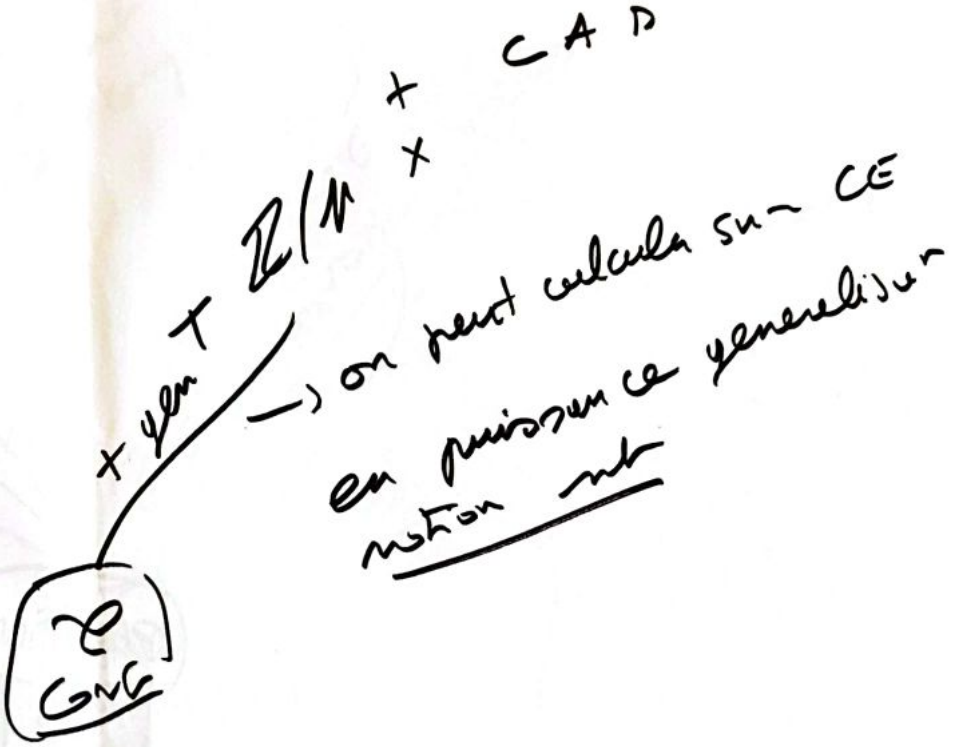
$a + c \equiv b + c \pmod n$

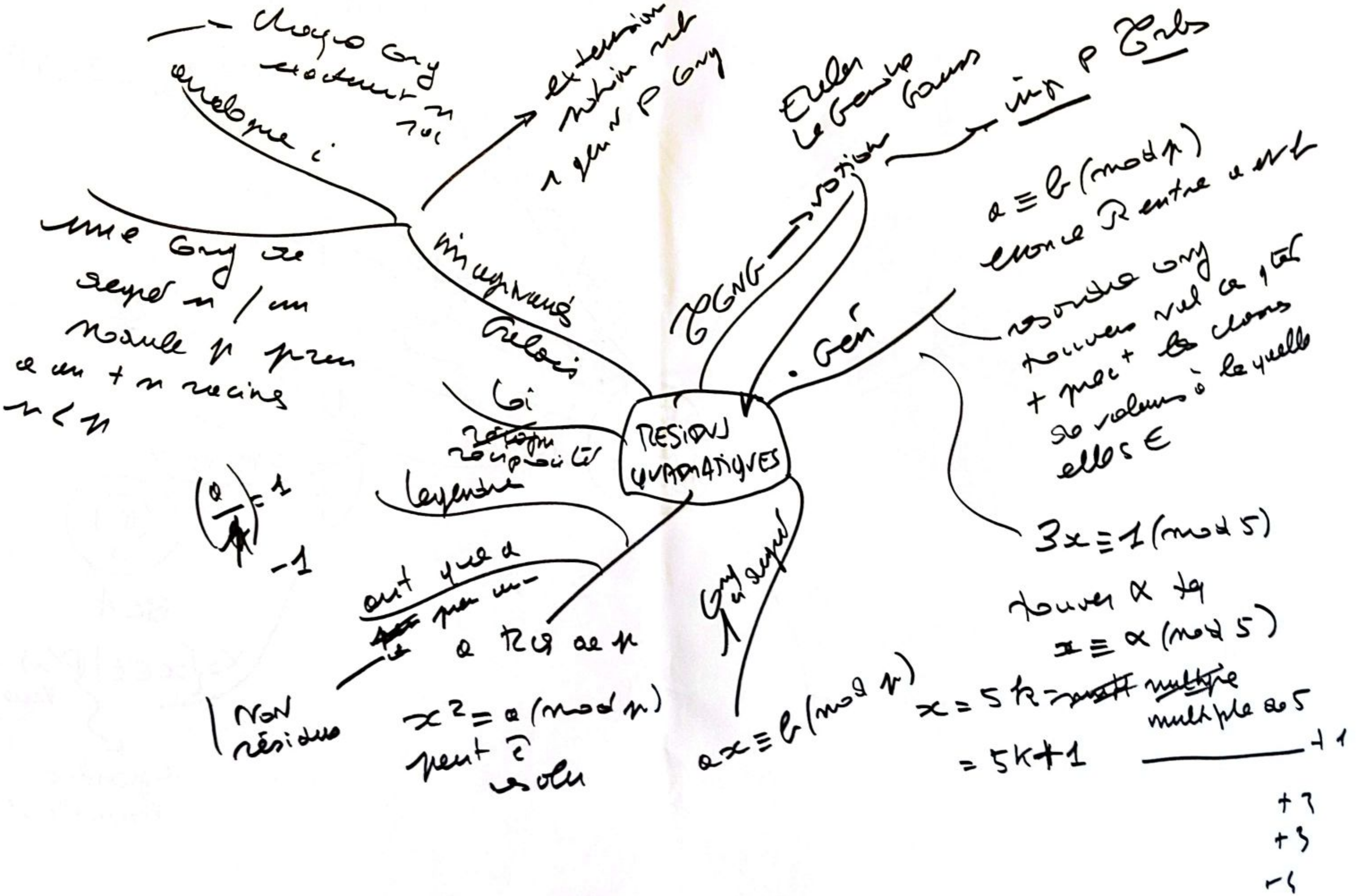
ac bc

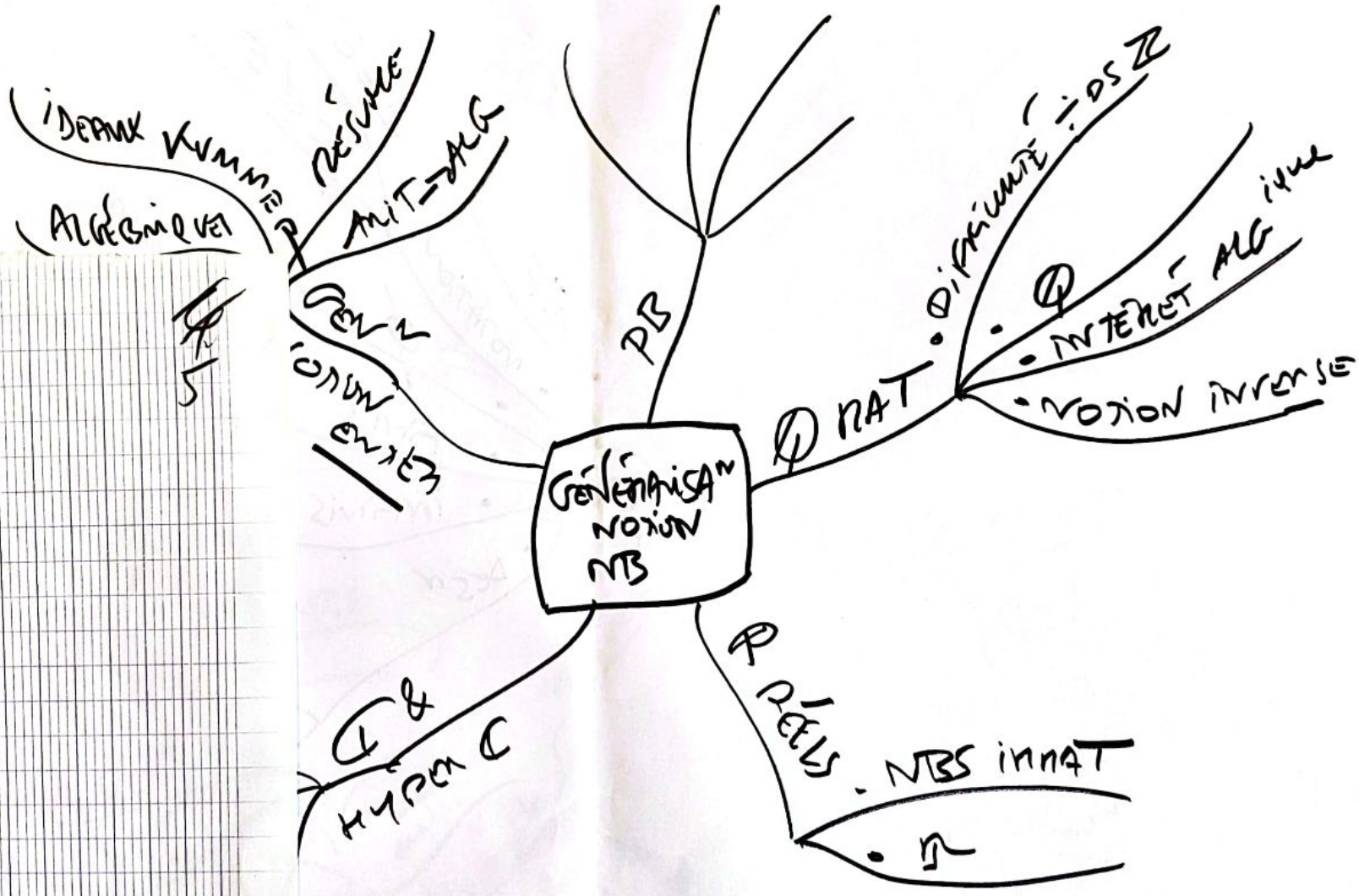
ac



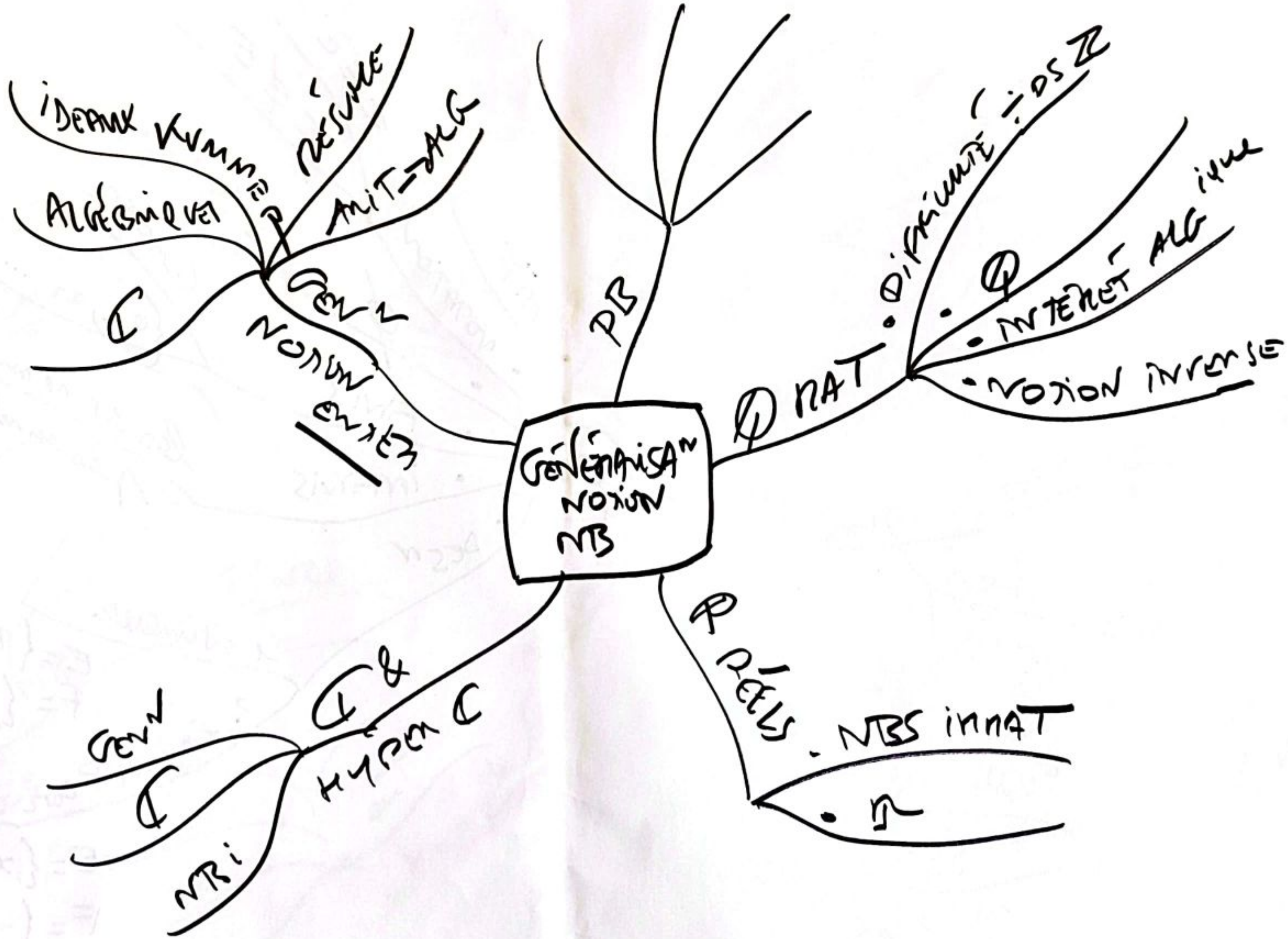
Calcul
sur CE
CEs de ℤ
+ plus T
x ≡ r (mod n)
peut prendre
0, 1, 2, 3 … n - 1
→ n classes
ℤ/2 (mod 2)
pairs & impairs
$\bar{0}+\bar{1}=\bar{1}+\bar{0}=\bar{1}$
$\bar{1}+\bar{1}=\bar{0}$
$\bar{0}+\bar{0}=\bar{0}$
pair + pair = pair
+ ×
$\bar{1}$
$\bar{0}$
15, 21, 27
dont ÷ par 6
classe $\bar{3}$
Ex
n = 6
ℤ/6
CR (mod 6)
$\{\bar{0}, \bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{3}\}$
$\bar{0}$
$\bar{1}$
$\bar{2}$
ces n classes =
classes résiduelles
(mod n)
noté
$ℤ/n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$

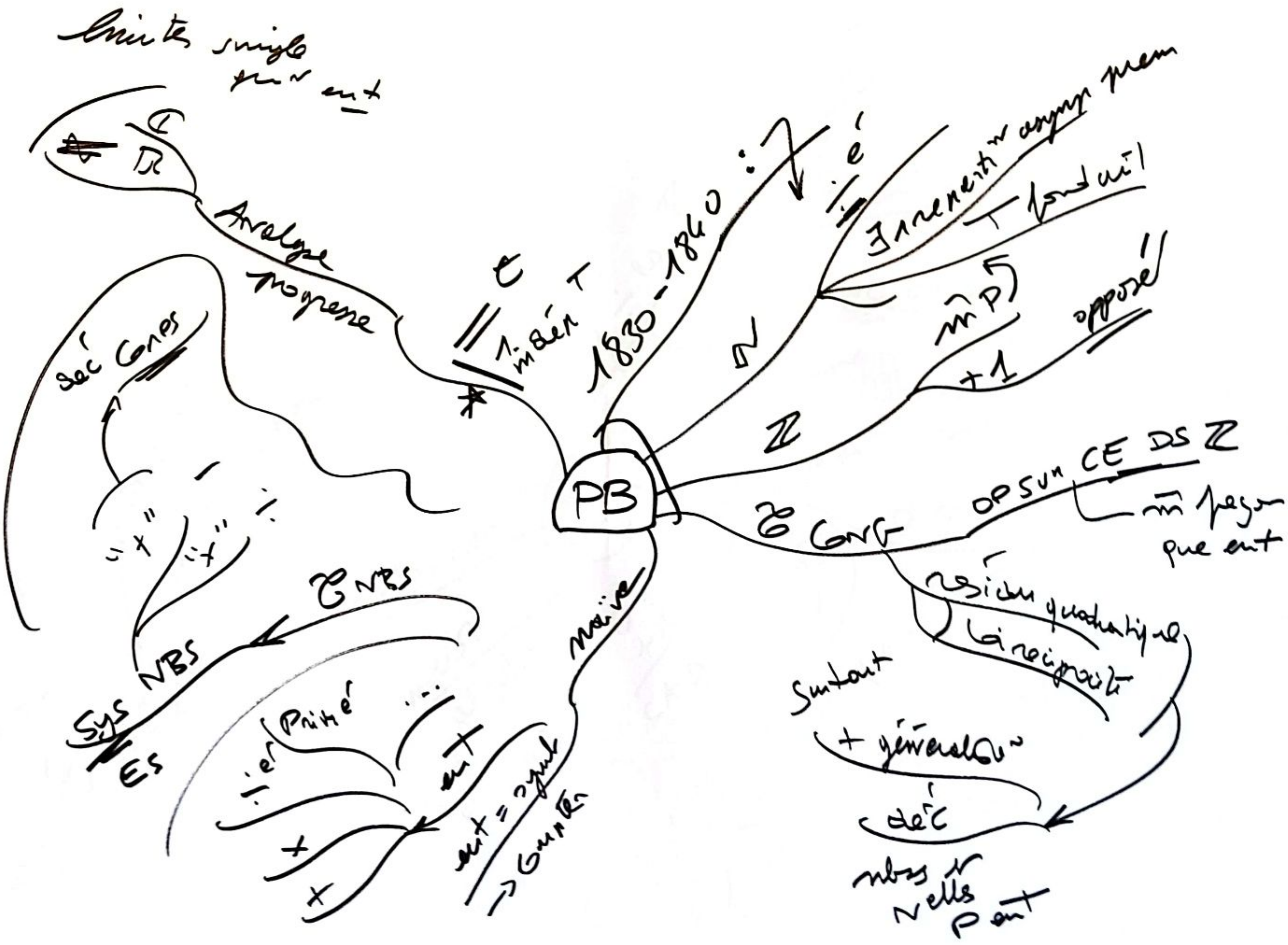

+ CAD
+ $\mathbb{Z}/n$
+ $\mathbb{Z}$
+ GMP
$\mathbb{Z}$
GMP
→ on peut calculer sur ce
en puissance généralisée
notion nouvelle

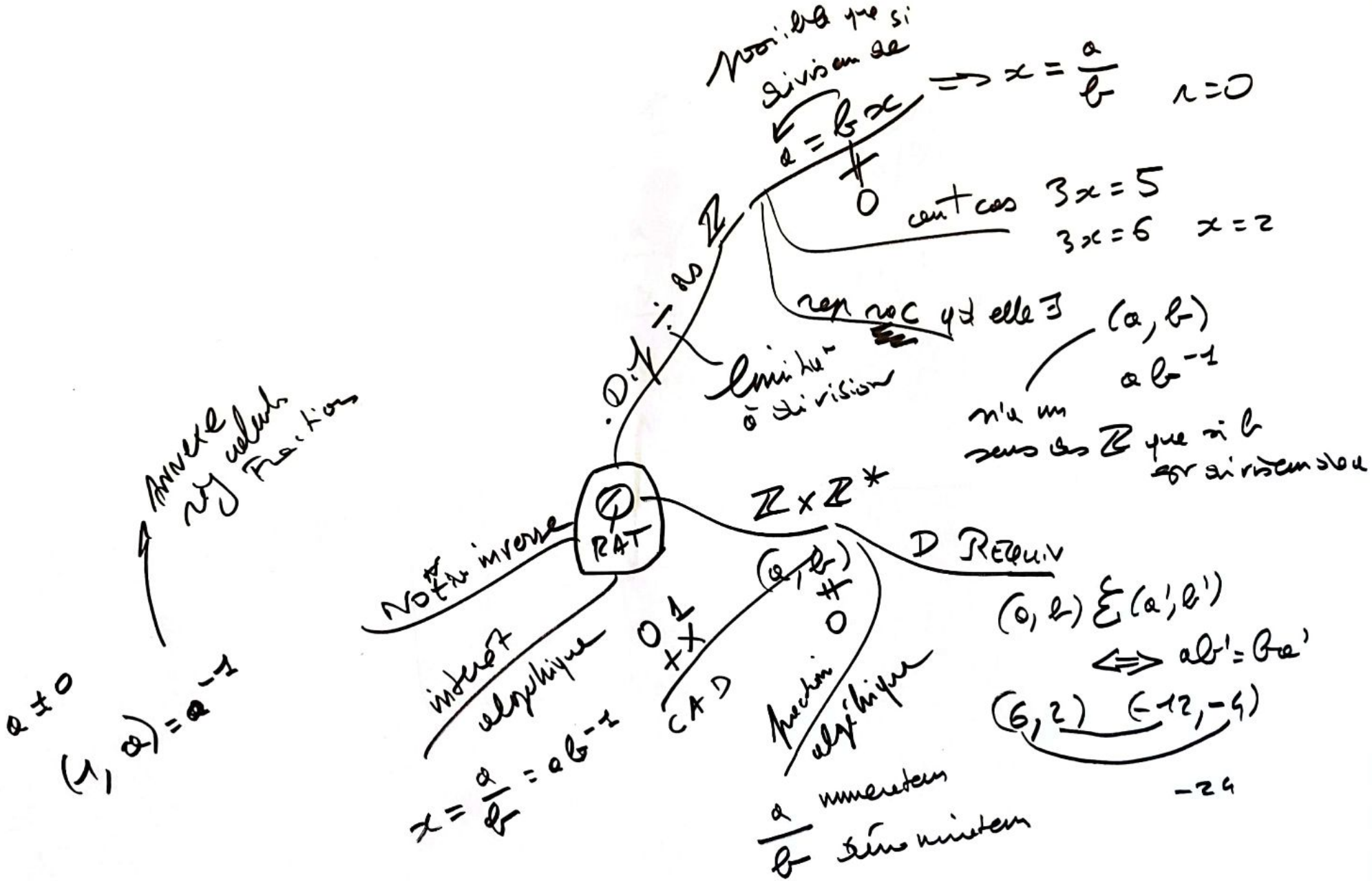

RÉSIDUS QUADRATIQUES
Gén
$a \equiv b \pmod p$
énonce R entre a et b
résoudre cong trouver val de x tel + précis les classes de valeurs à laquelle elles ∈
$3x \equiv 1 \pmod 5$
trouver α tq
$x \equiv \alpha \pmod 5$
$x = 5k$ multiple de 5
$= 5k+1$
+1
+2
+3
+4
notion
Euler
Legendre Gauss
Galois
loi de réciprocité
Legendre
$\left(\frac{a}{p}\right) = 1$
-1
a RQ de p
$x^2 \equiv a \pmod p$
peut ê résolu
Non résidus
$ax \equiv b \pmod p$
extension notion
une cong de degré n / un nombre p prem a au + n racines
$r < n$



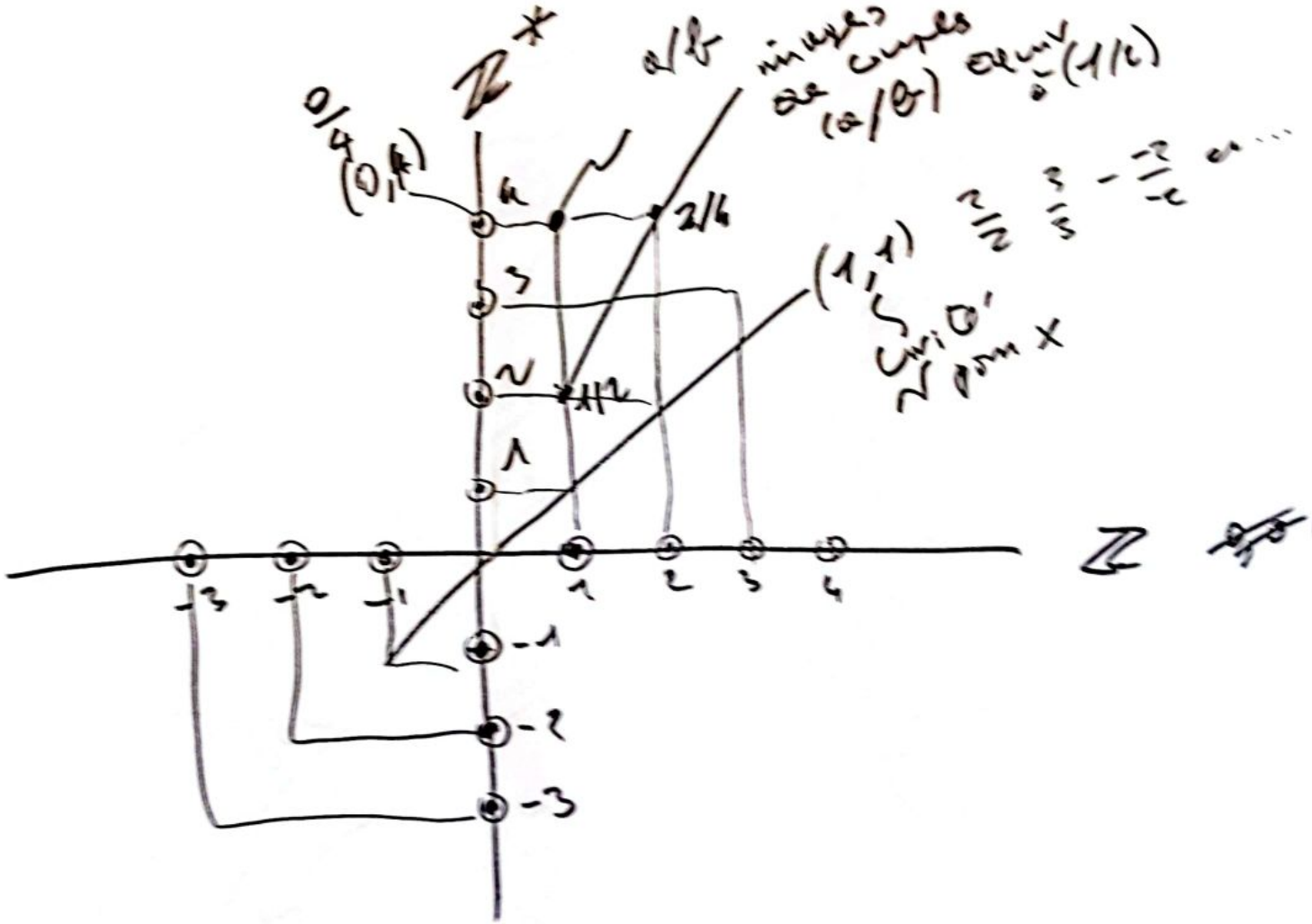
Cas col
généralisation
de la notion de nb

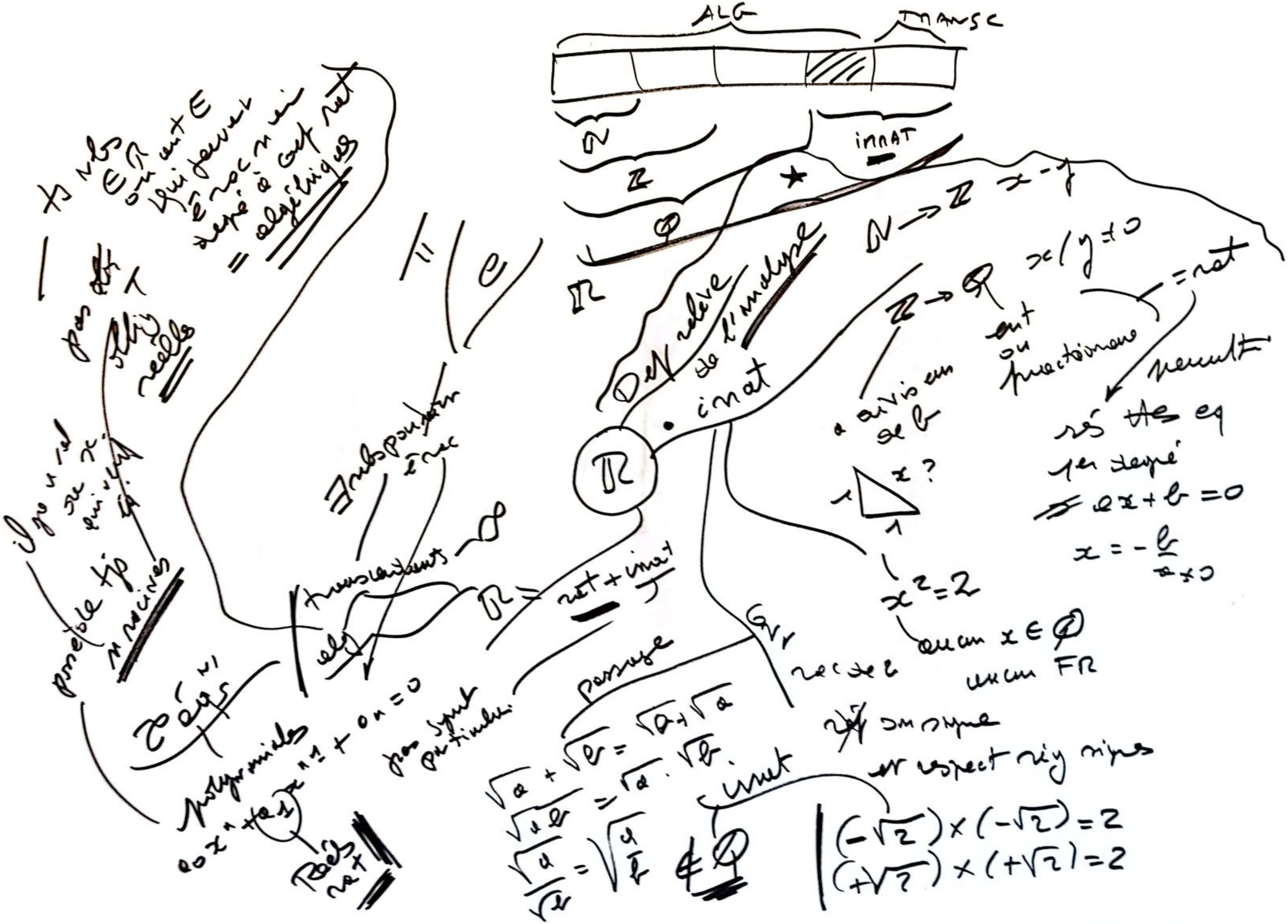

GÉNÉRALISATION NOTION NB
PB
NAT
• DIFFICULTÉ ÷ DS Z
• INTERNET ALG
• NOTION INVERSE
RÉELS
. NBS IRRAT
HYPER C
GÉNÉR
IDÉAUX
KUMMER
RÉSUMÉ
ALGÉBRIQUE
GÉNÉR
NOTION ENTIER


PB
Analyse
1830-1840
Sys NBS
ES
Privé
opposé
CE DS
Surtout

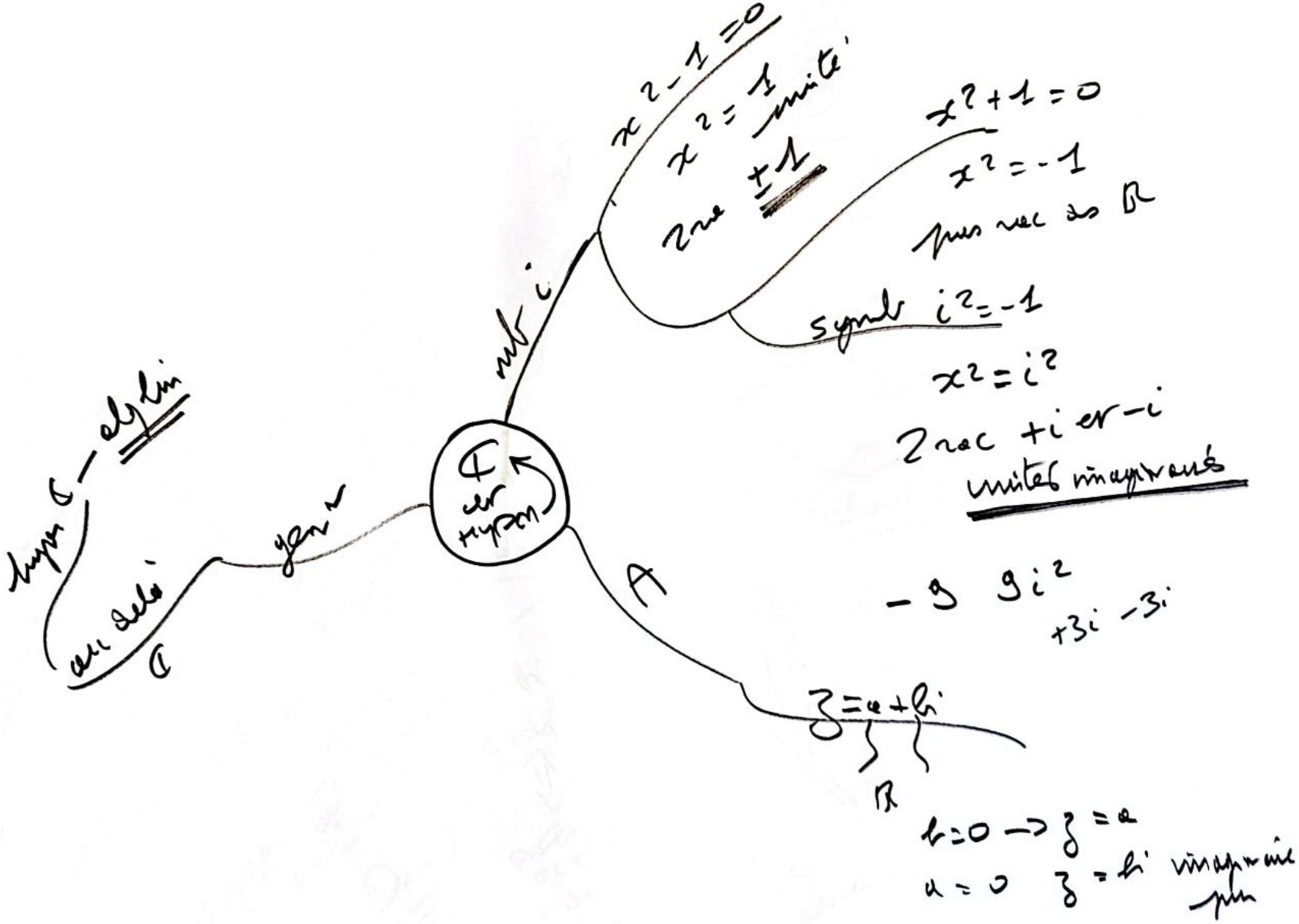

Possible que si
divisem de
$a = bx$
$\Rightarrow x = \frac{a}{b}$ $r = 0$
$\neq 0$
cont cas $3x = 5$
$3x = 6$ $x = 2$
rep nec y a elle ∃
(a, b)
ab^{-1}
n'a un
sens ds $\mathbb{Z}$ que si b
est inversable
$\mathbb{Z}$
$\mathbb{Z} \times \mathbb{Z}^*$
D Requiv
$(a, b) \mathcal{R} (a', b')$
$\Leftrightarrow ab' = ba'$
$(6, 2)$ $(-12, -4)$
-24
$\mathbb{Q}$
RAT
Notat inverse
$a \neq 0$
$(1, a) = a^{-1}$
Annule
les calculs
Fractions
interêt
algébrique
$x = \frac{a}{b} = ab^{-1}$
0 1
+ ×
CAD
(a, b)
$\neq$
0
fraction
algébrique
$\frac{a}{b}$ numérateur
dénominateur

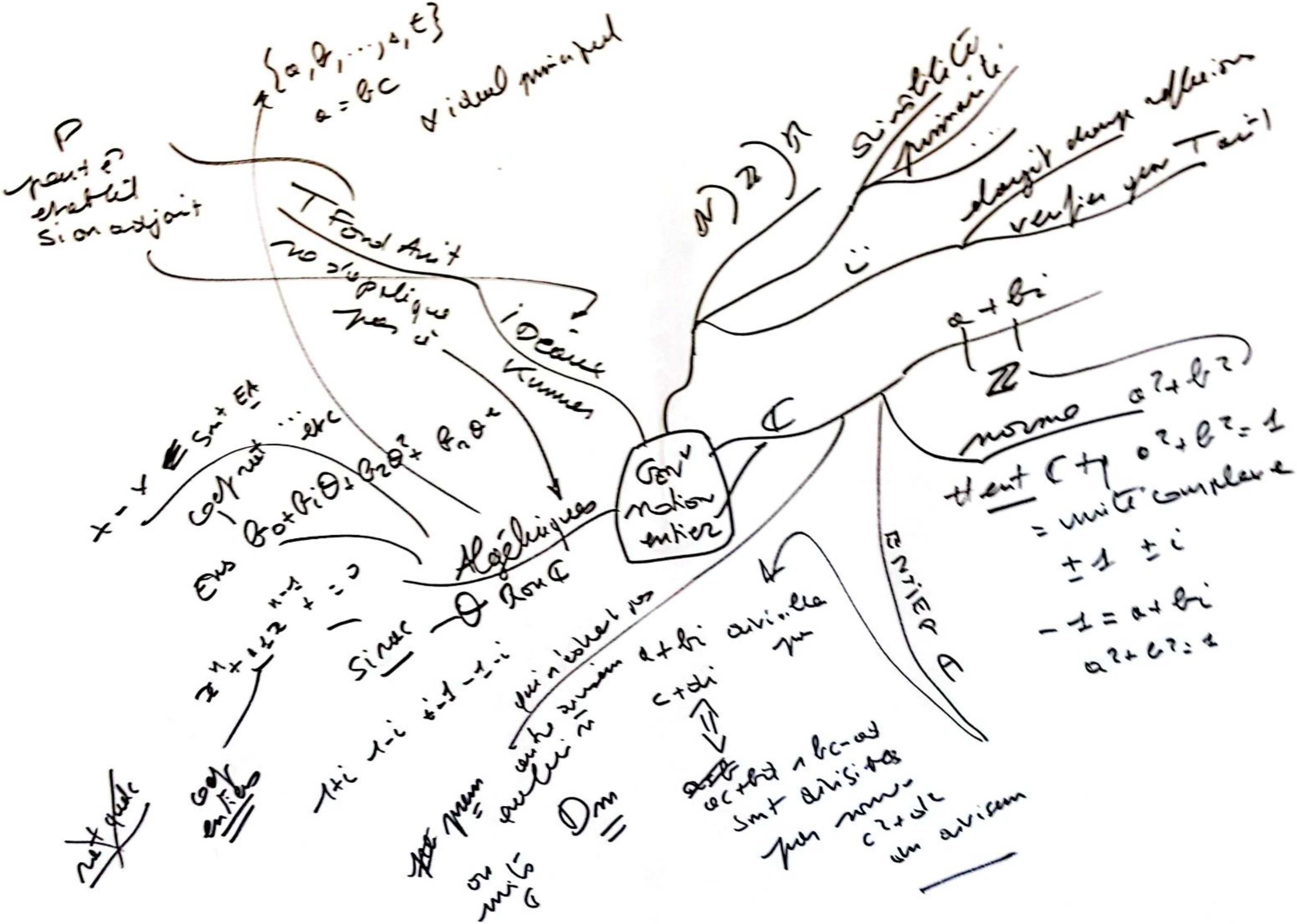
$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^*$

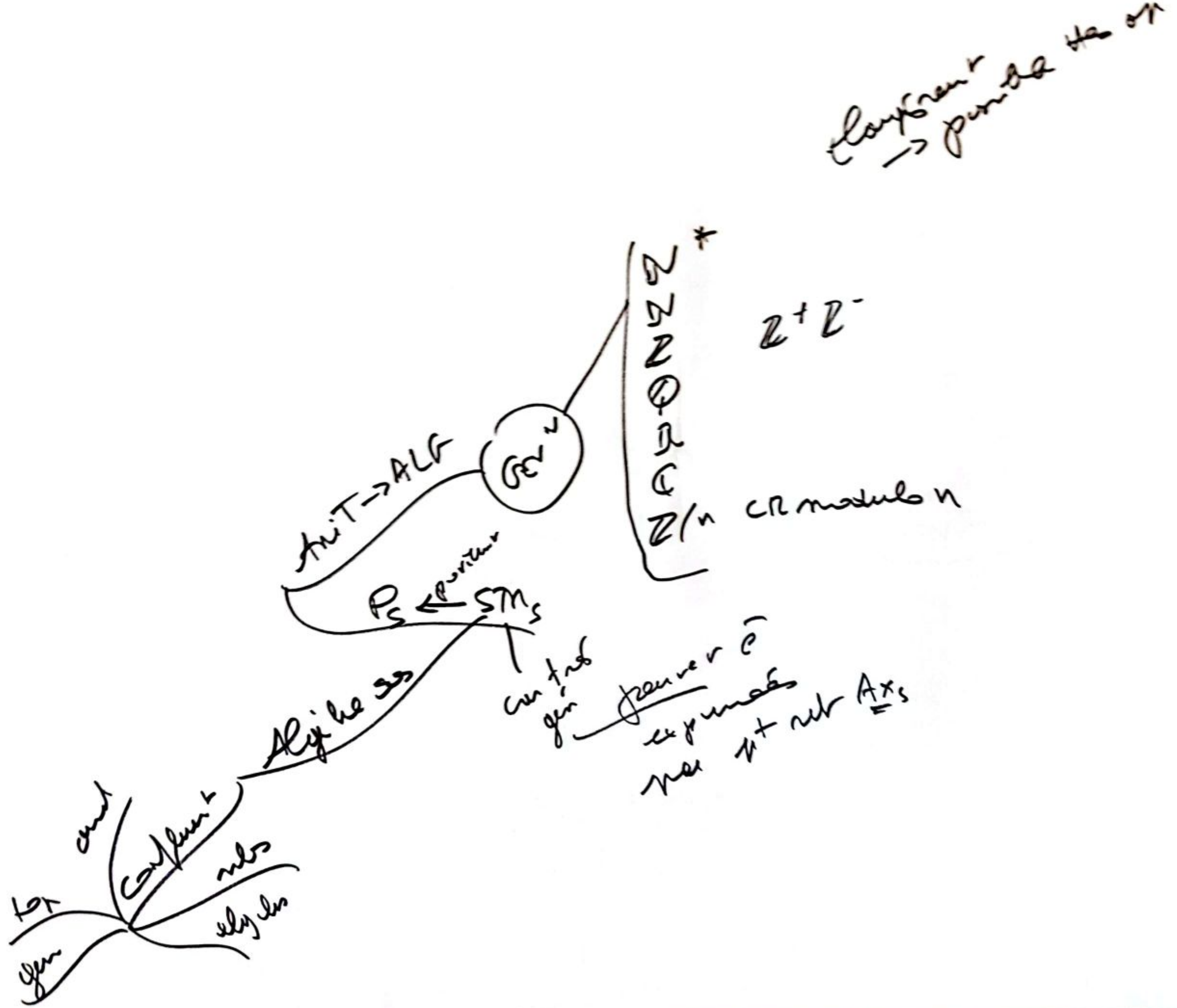




ALG
TRANSC
N
Z
Q
INNAT
R
π
e
N → Z x − y
x / y ≠ 0
Z → Q
= rat
résultats
rés des éq 1er degré
ax + b = 0
x = − b/a
a ≠ 0
Déf relève de l'analyse
irrat
R = rat + irrat
transcendants
x² = 2
aucun x ∈ Q
aucun FR
passage
polynomiales
√a + √b ≠ √(a+b)
√(ab) = √a · √b
√a / √b = √(a/b)
∉ Q
irrat
en respect des signes
(−√2) × (−√2) = 2
(+√2) × (+√2) = 2

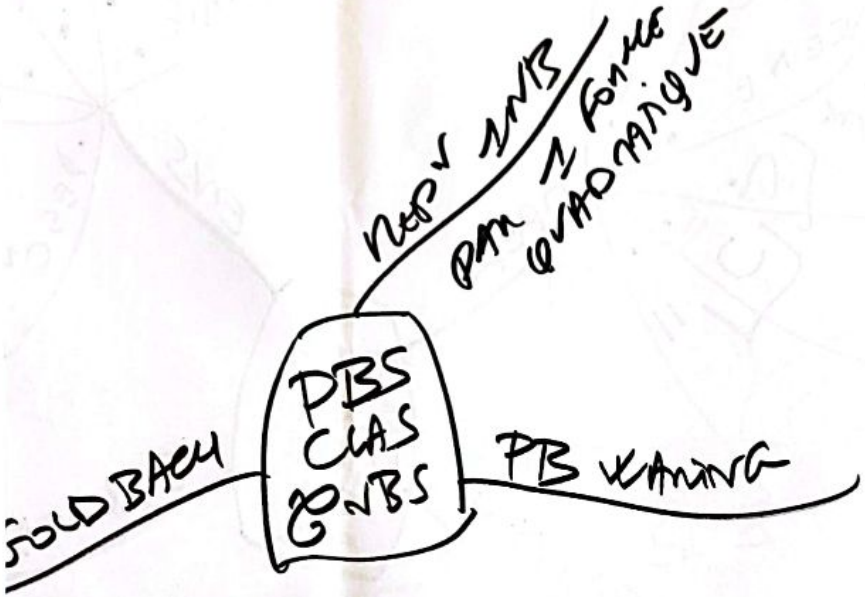

$x^2 - 1 = 0$
$x^2 = 1$
2 sol ±1
unité
$x^2 + 1 = 0$
$x^2 = -1$
pas réel dans ℝ
symb $i^2 = -1$
$x^2 = i^2$
2 sol +i et -i
unités imaginaires
mb i
ℂ
ens
ℂ - alg lin
ens des
ℂ
-9 $9i^2$
+3i -3i
$z = a + bi$
ℝ
$b = 0 \rightarrow z = a$
$a = 0$ $z = bi$ imaginaire pur


Gen^r notion entier
Algébriques
Idéaux Kummer
T Fond Arit
α idéal principal
α = bc
a + bi
ℤ
ℂ
norme a² + b²
a² + b² = 1
unité complexe
±1 ±i
−1 = a + bi
ENTIER A
1+i 1−i −1+i −1−i
c+di
Dm



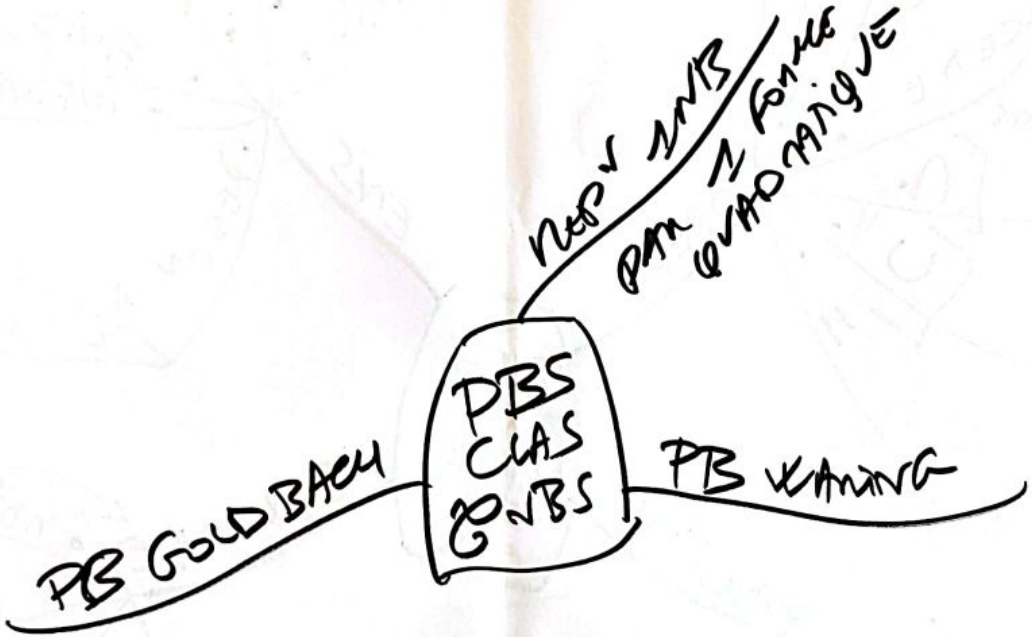
AniT -> ALG
GEV
Z/n CR modulo n
Algèbres

6



Cas col

Pbs classiques


PBS
CLAS
GNBS
PB GOLDBACH
PB KEARNS

Rep^n
1 NB
par 1
Forme quadratique

pol dont formes ts sur 2ème degré

Ex $x^2 - y^2$

$3x^2 - 5xy + z^2$ — 2ème somme

binaires deux indéterminées

$f = ax^2 + bxy + cy^2$

$\mathbb{R}$

$\mathbb{C}$

Si $\exists$ 2 ent $u \wedge v \neq 0$ tq

$m = au^2 + buv + cv^2$

m représenté par fq f

si a et premiers entre eux

rep^n est primitive

étude

Grand calcul

2G f.coef

Det $D = \frac{ac - b^2}{4}$

Disc $\Delta = -4D = b^2 - 4ac$

> 0

$+$

< 0

indéfinie

définie (+)

$ac \neq 0$

→ classe

transf lin

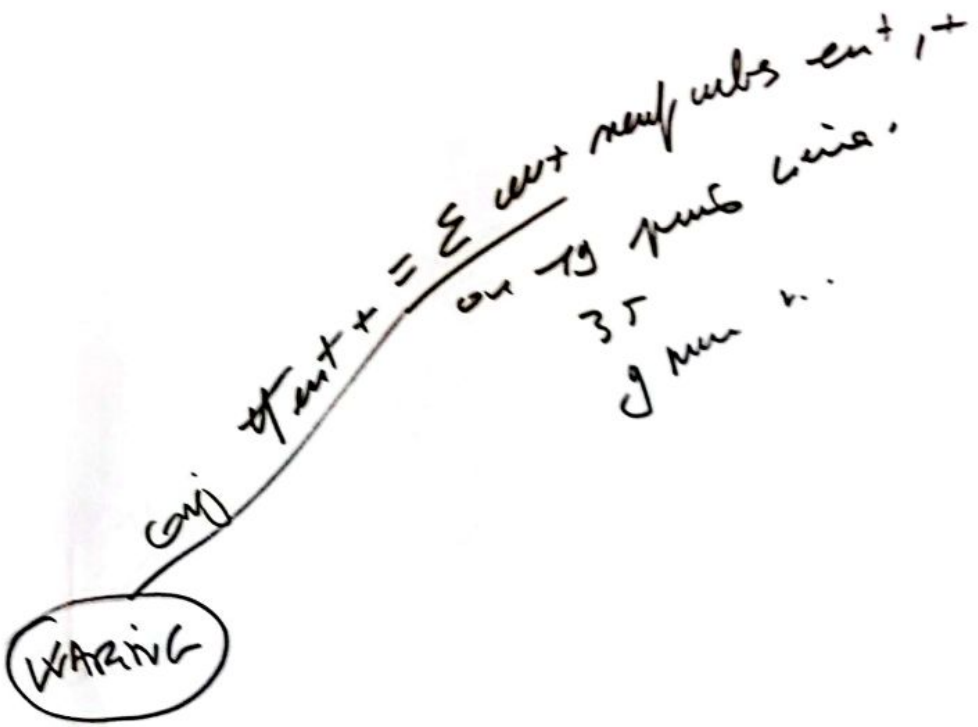
$x = \alpha x' + \beta y'$

$y = \gamma x' + \delta y'$

équivalente

tt fq

à une forme f'


WARING


GOLBACH
∀ ent Σ 3 nbs prem
pair Σ 2
conj