



[Retour vers le sommaire de la page sur les nombres décadiques](#)

## 11-Equations $x^n=x$ , $x^n=-x$ et $x^n=1$ ( cad racines nièmes de 1)

P11.0->  $n$  étant un entier naturel  $\geq 2$ , toute solution d'une des équations  $x^n=x$ ,  $x^n=-x$ ,  $x^n=1$ , dans NB(10), est obligatoirement entière décadique (ou brenom entier) (même raisonnement que celui fait pour l'équation  $x^2=x$  : voir chapitre 6).

Et de façon évidente

**Le produit de deux solutions de  $x^n=x$  est une solution de  $x^n=x$**

**Le produit de deux solutions de  $x^n=-x$  est une solution de  $x^n=x$**

**L'inverse d'une solution inversible de  $x^n=x$  est solution de  $x^n=x$**

**L'inverse d'une solution inversible de  $x^n=-x$  est solution de  $x^n=-x$**

Je ferai apparaître ici, en plus des propriétés P11.i, quelques résultats R11.i qui en fait, seront généralisés par P11.3, P11.4, P11.5.

R11.1-> **L'ensemble solution de  $x^2=x$  est  $S_2=\{0 ; 1 ; a ; b\}$  avec  $ab=0$ ,  $a+b=1$  (voir chapitre 6)**

R11.2-> **L'ensemble solution de  $x^2=-x$  est  $S_{-2}=\{0 ; -1 ; -a ; -b\}$**

C'est évident, car d'après R11.1, 0, 1, -a, -b sont quatre solutions distinctes de  $x^2=-x$ , et cf P8.10, ce sont les seules. Voir aussi l'exercice 14 du chapitre 9.

P11.0 se vérifie : le produit de deux éléments de  $S_{-2}$  est bien dans  $S_2$

R11.3-> **L'ensemble solution de  $x^3=x$  est  $S_3=\{0 ; -1 ; 1 ; -a ; a ; -b ; b ; a-b ; b-a\}$  : il y a neuf solutions**

dont les cinq derniers chiffres sont

0	.....00000
-1	.....99999
1	.....00001
-a	.....09375
a	.....90625
-b	.....90624
b	.....09376
a-b	.....81249
b-a	.....18751

Exercice 1 : prouver R11.3 (vérifier que ces neuf nombres sont solutions et utiliser P8.10)

**P11.1-> L'ensemble solution de  $x^3=-x$  est  $S_{-,3}=\{0 ; -c ; c\}$  avec  $c$  se terminant par .....186432,  $c^2=-b$  (donc  $-b$  a deux racines carrées  $-c$  et  $c$  d'après P9.3),  $ac=0$  (donc  $c$  est diviseur de 0 associé à  $a$ ),  $bc=c$   
rappel :  $-a$  n'a pas de racine carrée (voir P9.9)**

Remarque : il est assez facile de prouver que cette équation a au plus trois solutions. En effet, on a alors nécessairement  $(x^2)^2=-x^2$ , donc  $x^2=0$  ou  $-1$  ou  $-a$  ou  $-b$  ; or 0 a une seule racine carrée qui est 0,  $-1$  et  $-a$  n'ont pas de racine carrée (voir P9.4 et P9.9), et  $-b$  en a au plus deux (cf P9.3). Donc  $x^3=-x$  a au plus trois solutions 0 (effectivement solution) et éventuellement les racines carrées de  $-b$ , si ... elles existent et si elles vérifient effectivement  $x^3=-x$ !

Exercice 2 : prouver P11.1 en utilisant les congruences pour justifier l'existence de trois solutions uniquement et pour en donner des valeurs approchées. On pourra s'inspirer du début de l'exercice du chapitre 6 sur  $x^2=x$ .

Exercice 3 :

- 1) Peut-on trouver deux nombres décadiques  $x$  et  $y$  non nuls tels que  $x^2+y^2=0$ ?
- 2) Montrer que si deux nombres décadiques  $x$  et  $y$  non nuls vérifient  $x^2+y^2=0$ , alors ce sont des diviseurs de 0 non associés, mais associés à un même 3ième.

**P11.2-> L'ensemble solution de  $x^5=x$  est  $S_5=\{0 ; -1 ; 1 ; -a ; a ; -b ; b ; a-b ; b-a ; -c ; c ; -a-c ; -a+c ; a-c ; a+c\}$  : il y a quinze solutions.**

les cinq derniers chiffres des six dernières solutions sont

$-c$	.....13568
$c$	.....86432
$-a-c$	.....22943
$-a+c$	.....95807
$a-c$	.....04193
$a+c$	.....77057

On notera que parmi ces quinze solutions, six sont des diviseurs de 0 ( $-a$ ,  $a$ ,  $-b$ ,  $b$ ,  $-c$ ,  $c$ ) et huit sont inversibles ( $-1$ ,  $1$ ,  $a-b$ ,  $b-a$ ,  $-a-c$ ,  $-a+c$ ,  $a-c$ ,  $a+c$ ).

**L'ensemble des carrés de ces quinze solutions est  $\{0 ; 1 ; a ; b ; -b ; a-b\} \subset S_5$ .**

On retrouve, cf P11.0, que  $S_5$  est stable par élévation au carré.

**L'ensemble des racines carrées de ces quinze solutions redonne exactement l'ensemble de ces quinze solutions.**

$S_5$  est donc stable par racine carrée.

Précisons :

$s \in S_5$	racines carrées de $s$
0	0
1	{ $-1 ; 1 ; a-b ; b-a$ }

$$a \quad \{-a ; a\}$$

$$-b \quad \{-c ; c\}$$

$$b \quad \{-b ; b\}$$

$$a-b \quad \{-a+c ; -a-c ; a-c ; a+c\}$$

les neuf autres éléments de  $S_5$   
n'ont pas de racine carrée

Exercice 4 : prouver P11.2 (remarquer que  $x^5=x \Rightarrow x^6=x^2$ ).

Exercice 5 : montrer que l'ensemble solution de  $x^5=-x$  est  $S_{-,5}=\{0\}$

**P11.3-> Pour tout entier  $p \geq 1$ , l'ensemble solution de l'équation  $x^{2p}=x$  est  $S_{2p}=S_2=\{0 ; 1 ; a ; b\}$ .**

**En particulier,  $S_4=S_2$ .**

Exercice 6 : prouver P11.3 (par les congruences, en s'inspirant de la preuve de R11.4 ; mais je suis tombé sur une difficulté lorsque  $2p-1 \equiv 5 \pmod{10}$ , et donc dans ce cas ma solution est un peu "longuette" : désolé mais je n'ai pas trouvé mieux. En tout cas, c'est la seule démonstration vraiment longue de cette page).

Exercice 7 : déterminer l'ensemble solution  $S_7$  de  $x^7=x$ , en utilisant  $S_4$ , donné par P11.3.

**P11.4-> Soit  $n$  un entier naturel  $\geq 2$ , et  $S_n$  l'ensemble solution de l'équation (dans NB (10))  $x^n=x$ .**

**Alors pour tout entier naturel  $n \geq 2$  on a  $S_n \subset S_5$ , cad toute solution de  $x^n=x$  est une solution de  $x^5=x$ .**

**De façon plus précise :**

**si  $n$  est pair, alors  $S_n=S_2=\{0 ; 1 ; a ; b\}$**

**si  $n \equiv 3 \pmod{4}$  alors  $S_n=S_3=\{0 ; -1 ; 1 ; -a ; a ; -b ; b ; a-b ; b-a\}$**

**si  $n \equiv 1 \pmod{4}$  alors  $S_n=S_5=\{0 ; -1 ; 1 ; -a ; a ; -b ; b ; a-b ; b-a ; -c ; c ; -a-c ; -a+c ; a-c ; a+c\}$**

Remarque :  $x^n=x$  et  $x$  inversible entraîne  $x^{n-1}=1$ , c'est-à-dire  $x$  est une racine  $(n-1)$ ième de 1. Voir P11.6 pour une étude complète de cet aspect.

Exercice 8 : prouver P11.4 (cela peut être fait sans congruences, en utilisant notamment certains des résultats ci-dessus).

**P11.5-> Soit  $n$  un entier naturel  $\geq 2$ , et  $S_{-,n}$  l'ensemble solution de l'équation (dans NB (10))  $x^n=-x$ .**

**Alors pour tout entier naturel  $n \geq 2$  on a  $S_{-,n} \subset S_5$ , cad toute solution de  $x^n=-x$  est une solution de  $x^5=x$ .**

**De façon plus précise :**

si  $n$  est pair, alors  $S_{-,n}=S_{-,2}=\{-1 ; 0 ; -a ; -b\}$

si  $n \equiv 3 \pmod{4}$  alors  $S_{-,n}=S_{-,3}=\{0 ; -c ; c\}$

si  $n \equiv 1 \pmod{4}$  alors  $S_{-,n}=S_{-,5}=\{0\}$

Exercice 9 : prouver P11.5

P11.6-> Soit  $n$  un entier  $\geq 1$ .

L'ensemble des racines nièmes de 1, dans  $NB(10)$ , est

si  $n$  impair,  $\{1\}$

si  $n \equiv 2 \pmod{4}$ ,  $\{-1 ; 1 ; a-b ; b-a\}$

si  $n \equiv 0 \pmod{4}$ ,  $\{-1 ; 1 ; a-b ; b-a ; -a-c ; -a+c ; a-c ; a+c\}$

Remarque 1 :

on peut vérifier que dans chacun de ces trois cas, l'ensemble des racines nièmes de 1 est bien un groupe multiplicatif. Pour  $n$  pair il ne s'agit pas de groupes cycliques : pour  $n \equiv 2 \pmod{4}$ , il s'agit d'un groupe de Klein (tous les éléments autres que 1 sont d'ordre 2), pour  $n \equiv 0 \pmod{4}$ , les quatre derniers éléments du groupe sont d'ordre 4.

Remarque 2 :

l'ensemble des racines nièmes de 1, lorsque  $n$  décrit  $\mathbb{N}^*$  est l'ensemble des éléments inversibles de  $S_5$  (voir P11.2).

Exercice 10 : prouver P11.6

## Solution des exercices du chapitre 9

### Exercice 1

Puisque  $x^2=x$  entraîne que  $x^n=x$  pour tout  $n \geq 2$ , les quatre solutions 0, 1, a, b de  $x^2=x$  sont solutions de  $x^3=x$ .

Donc -1, -a, -b sont aussi solutions de  $x^3=x$ .

Enfin,  $x^2=1$  entraîne que  $x^3=x$  et donc a-b et b-a (dont les carrés sont égaux à 1, cf P9.1) sont aussi solutions de  $x^3=x$ .

On a donc trouvé neuf solutions distinctes (par exemple on examine les deux derniers chiffres de leurs développement décadique) pour l'équation  $x^3=x$ , donc ce sont les seules d'après P8.10.

autre façon :  $x^3=x \Rightarrow (x^2)^2=x^2$ , et donc  $x^2=0$  ou 1 ou a ou b, ce qui donne que nécessairement  $x=0$  ou -1 ou 1 ou a-b ou b-a ou -a ou a ou -b ou b (voir P9.3 pour les racines carrées de a et b, voir P9.1 pour celles de 0, 1, voir P9.4 pour -1).

Réciproquement, ces au plus neuf possibilités distinctes pour x sont effectivement solutions de  $x^3=x$ , puisque notamment  $(a-b)^3=a^3-b^3=a-b$ . Et toujours d'après P8.10 ce sont les seules.

### Exercice 2

Ce cas est moins immédiat, car tout simplement les solutions font intervenir un entier décadique que l'on n'a pas encore rencontré.

On s'inspire donc de la méthode utilisée pour l'équation  $x^2=x$  (voir chapitre 6).

Je ne reprends pas toutes les justifications :

**x solution de  $x^3=-x \Leftrightarrow x$  est entier décadique et pour tout  $n \geq 0$ ,  $([x]_n)^3 \equiv -[x]_n \pmod{10^{n+1}}$ . Cette congruence sera appelée la relation  $P_n$ .**

$P_0$  donne  $(x_0)^3 \equiv -x_0 \pmod{10}$ , ce qui donne comme uniques possibilités pour  $x_0$  : 0, 2, 3, 5, 7, 8.

$P_0$  étant vérifiée,  $P_1$  donne  $(10x_1+x_0)^3 \equiv -10x_1-x_0 \pmod{100}$ , soit  $(3x_0^2+1)x_1+r_0 \equiv 0 \pmod{10}$  avec  $r_0 = (x_0^3+x_0)/10$  (licite, car  $P_0$  est vérifiée).

On constate alors que

si  $x_0=3$  alors  $r_0=3$  et on doit avoir  $28x_1+3 \equiv 0 \pmod{10}$ , ce qui est impossible, le membre de gauche étant impair

si  $x_0=5$  alors  $r_0=13$  et on doit avoir  $76x_1+13 \equiv 0 \pmod{10}$ , ce qui est impossible, le membre de gauche étant impair

si  $x_0=7$  alors  $r_0=35$  et on doit avoir  $148x_1+35 \equiv 0 \pmod{10}$ , ce qui est impossible, le membre de gauche étant impair

Par contre, pour  $x_0=0$  ou 2 ou 8, on n'a pas d'impossibilité au niveau de  $x_1$ .

**Les seules possibilités pour  $x_0$  sont donc 0, 2, 8.**

On peut montrer tout de suite que **l'équation  $x^3 \equiv -x$  admet une seule solution se terminant par 0 : c'est 0.**

En effet, soit  $x$  une solution se terminant par  $x_0=0$  et qui soit non nulle ; alors elle admet au moins un chiffre de rang  $\geq 1$  qui soit non nul. Soit  $k$  le rang minimum d'un chiffre non nul : donc  $[x]_k = x_k 10^k$ , avec  $x_k \neq 0$  et  $k \geq 1$ .

La relation  $P_k$  devant être vérifiée,  $10^{3k}(x_k)^3 \equiv -10^k x_k \pmod{10^{k+1}}$  ; or  $3k \geq k+1$  (puisque  $k \geq 1$ ) et donc 10 doit diviser  $x_k$ , ce qui est impossible puisque  $x_k \in \{1; 2; \dots; 9\}$ . Donc si  $x$  se termine par 0 et est solution, nécessairement c'est 0, qui est effectivement solution.

On va montrer maintenant que l'équation  $x^3 \equiv -x$  admet une et une seule solution se terminant par 2 et une et une seule solution se terminant par 8, ces deux solutions étant opposées.

**On pose, pour  $n \in \mathbb{N}$ ,  $r_n = (([x]_n)^3 + [x]_n) / 10^{n+1}$  et  $w_{n+1}$  = le chiffre de rang  $n+1$  de  $([x]_n)^3$ . Si  $x_0 \neq 0$  et si  $P_n$  est vraie, alors  $r_n \in \mathbb{N}$  et  $r_n \equiv w_{n+1} + 1 \pmod{10}$ .**

En effet, on a  $([x]_n)^3 + [x]_n = 10^{n+1} r_n$  avec  $r_n$  dans  $\mathbb{N}$ , puisque  $P_n$  est vérifiée, et on peut écrire  $([x]_n)^3 = A \times 10^{n+1} + B$ , avec  $B$  entier constitué des  $n+1$  derniers chiffres de  $([x]_n)^3$  et  $A \equiv w_{n+1} \pmod{10}$ , puisque par définition,  $w_{n+1}$  est le dernier chiffre de  $A$ .

Donc  $A \times 10^{n+1} + B + [x]_n = r_n 10^{n+1}$  et ainsi  $10^{n+1}$  divise  $B + [x]_n$ , soit  $B + [x]_n = K \times 10^{n+1}$ , avec  $K$  dans  $\mathbb{N}$ .

Mais,  $0 \leq B + [x]_n \leq 2(10^{n+1} - 1)$ , donc  $K=0$  ou 1. Mais  $K=0$  donne  $B + [x]_n = 0$ , donc  $[x]_n = 0$  (puisque  $B$  et  $[x]_n$  sont  $\geq 0$ ), ce qui est impossible car  $x_0 \neq 0$ . Donc  $K=1$  et  $A \times 10^{n+1} + 10^{n+1} = r_n 10^{n+1}$ , soit  $A+1 = r_n$ , et donc  $r_n \equiv w_{n+1} + 1 \pmod{10}$ .

Remarque : si  $x_0=0$ , on ne peut exclure la possibilité  $[x]_n=0$ , et dans ce cas d'ailleurs,  $([x]_n)^3=0$ , donc  $w_{n+1}=0$ , tout comme  $r_n=0$  :  $r_n = w_{n+1} (=0)$ .

C'est pour cela que j'ai traité à part le cas  $x_0=0$ .

Pour  $n \in \mathbb{N}^*$ ,  $P_n$  sera vérifiée si et seulement si  $(10^n x_n + [x]_{n-1})^3 \equiv -10^n x_n - [x]_{n-1} \pmod{10^{n+1}}$ , ce qui équivaut à  $10^n(3([x]_{n-1})^2 + 1)x_n + ([x]_{n-1})^3 + [x]_{n-1} \equiv 0 \pmod{10^{n+1}}$ .

Cela exige que  $10^n$  divise  $([x]_{n-1})^3 + [x]_{n-1}$ , donc que  $P_{n-1}$  soit vraie, et alors

$([x]_{n-1})^3 + [x]_{n-1} = 10^n r_{n-1}$ , avec  $r_{n-1}$  entier naturel.

Donc  $x$  vérifie  $P_n \Rightarrow x$  vérifie  $P_{n-1}$  et  $(3([x]_{n-1})^2 + 1)x_n + r_{n-1} \equiv 0 \pmod{10}$

Réciproquement, si on a ces deux conditions, en multipliant la 2ième par  $10^n$ , on voit que  $x$

vérifie  $P_n$ .

Donc  $x$  vérifie  $P_n \Leftrightarrow x$  vérifie  $P_{n-1}$  et  $(3([x]_{n-1})^2+1)x_n+r_{n-1} \equiv 0 \pmod{10}$  (10)

Comme par ailleurs  $[x]_{n-1} \equiv x_0 \pmod{10}$  (10)

**Pour tout  $n$  dans  $\mathbb{N}^*$ ,  $x$  vérifie  $P_n \Leftrightarrow x$  vérifie  $P_{n-1}$  et  $(3x_0^2+1)x_n \equiv -r_{n-1} \pmod{10}$  (10)**

Enfin, dans le cas  $x_0 \neq 0$ ,  $P_{n-1}$  vérifiée entraînant  $r_{n-1} \equiv w_n+1 \pmod{10}$  (10), on peut écrire aussi

**Lorsque  $x_0 \neq 0$ ,**

**pour tout  $n$  dans  $\mathbb{N}^*$ ,  $x$  vérifie  $P_n \Leftrightarrow x$  vérifie  $P_{n-1}$  et  $(3x_0^2+1)x_n \equiv -(w_n+1) \pmod{10}$  (10)**

Donc, puisque  $x^3 = -x \Rightarrow$  que pour tout  $n$  dans  $\mathbb{N}$ ,  $P_n$  est vraie, c'est que  $x^3 = -x$  et  $x_0 \neq 0 \Rightarrow x_0 = 2$  ou  $8$  et pour tout  $n$  dans  $\mathbb{N}^*$ ,  $(3x_0^2+1)x_n \equiv -(w_n+1) \pmod{10}$  ;

Réciproquement si on a  $x_0 = 2$  ou  $8$  et pour tout  $n$  dans  $\mathbb{N}^*$ ,  $(3x_0^2+1)x_n \equiv -(w_n+1) \pmod{10}$  (10), alors,  $P_0$  est vraie, et comme  $(3x_0^2+1)x_1 \equiv -(w_1+1) \pmod{10}$  (10), c'est que  $P_1$  est vraie.

Et comme  $(3x_0^2+1)x_2 \equiv -(w_2+1) \pmod{10}$  (10), c'est que  $P_2$  est vraie.

Etc : pour tout  $n$  dans  $\mathbb{N}$ , on a  $P_n$  vraie, donc  $x^3 = -x$ .

**Finalement :  $x^3 = -x$  et  $x_0 \neq 0 \Leftrightarrow x_0 = 2$  ou  $8$  et pour tout  $n$  dans  $\mathbb{N}^*$ ,  $(3x_0^2+1)x_n \equiv -(w_n+1) \pmod{10}$  (10)**

On voit alors tout de suite que si  $3x_0^2+1$  est inversible modulo 10 (cad s'il est premier avec 10) alors  $x_n$  va exister et sera unique, et donc il existera un et un seul  $x$  (entier décadique) solution de  $x^3 = -x$  et dont le terme de rang 0 sera cet  $x_0$ .

**si  $x_0 = 2$ ,  $3x_0^2+1 = 13 \equiv 3 \pmod{10}$  et donc d'inverse 7 modulo 10 :  $x_n \equiv -7(w_n+1) \equiv 3(w_n+1) \pmod{10}$   
donc il existe une seule solution de  $x^3 = -x$  avec  $x_0 = 2$  : **elle sera notée  $c$****

**si  $x_0 = 8$ ,  $3x_0^2+1 = 193 \equiv 3 \pmod{10}$  et donc d'inverse 7 modulo 10 :  $x_n \equiv 3(w_n+1) \pmod{10}$   
donc il existe une seule solution de  $x^3 = -x$  avec  $x_0 = 8$  ; c'est forcément  $-c$ ,  
puisque  $c$  étant solution,  $-c$  est aussi solution et  $-c$  commence par 8.**

Remarque : à partir du moment où l'on sait qu'il existe une seule solution se terminant par 2, on peut en déduire tout de suite qu'il existe une seule solution se terminant par 8. En effet si  $x$  et  $x'$  sont deux solutions se terminant par 8,  $-x$  et  $-x'$  sont encore deux solutions, mais qui se terminent par 2, donc  $-x = -x'$  et  $x = x'$ .

**On a donc montré que l'équation  $x^3 = -x$  a exactement trois solutions :**

**0,  $-c$  (qui se termine par 8),  $c$  (qui se termine par 2).**

Déterminons les derniers chiffres de la solution  $c$ , celle commençant par 2.

Cf ci-dessus,  $x_n \equiv 3(w_n+1) \pmod{10}$  (10), ce qui va permettre le calcul des  $x_n$ , de proche en proche.

Mais comme  $P_{n-1}$  est forcément vérifiée ( $c$  est solution) on peut aussi dire

$$x_n \equiv 3((x]_{n-1})^3 + [x]_{n-1}) / 10^n \pmod{10} \text{ (10).}$$

C'est alors une question de choix personnel : soit on calcule  $([x]_{n-1})^3$  et on cherche son chiffre de rang  $n$  qui est  $w_n$ , soit on calcule  $(([x]_{n-1})^3 + [x]_{n-1}) / 10^n$  : c'est le choix que j'ai adopté ci-dessous (mais le lecteur peut essayer l'autre choix).

$$x_0 = 2 \text{ donne } x_1 \equiv 3(2^3+2)/10 \equiv 3 \pmod{10} \text{ et } x_1 = 3$$

$$x_1 = 3 \text{ donne } x_2 \equiv 3(32^3+32)/100 \equiv 3 \times 328 \equiv 3 \times 8 \equiv 4 \pmod{10} \text{ et } x_2 = 4$$

$$x_2 = 4 \text{ donne } x_3 \equiv 3(432^3+432)/1000 \equiv 3 \times 80622 \equiv 3 \times 2 \equiv 6 \pmod{10} \text{ et } x_3 = 6$$

$x_3=6$  donne  $x_4=3(6432^3+6432)/10000=3\times 26609586=3\times 6=8$  (10) et  $x_4=8$   
 $x_4=8$  donne ...  $x_5=1$ .

**Montrons que  $c^2=-b$  :**

$c^4=-c^2$  donc  $c^2$  est solution de  $x^2=-x$  et donc (voir R11.2)  $c^2=0$  ou  $-1$  ou  $-a$  ou  $-b$  ; mais  $c^2$  se termine par 4 alors que 0,  $-1$ ,  $-a$ ,  $-b$  se terminent respectivement par 0, 9, 5, 4 : donc la seule possibilité est  $c^2=-b$ .

Remarque :  $186432^2$  se termine bien par 890624, les six derniers chiffres de  $-b=a-1$ .

**Montrons que  $ac=0$  et  $bc=c$  :**

$c^3=-c$  s'écrit  $c\times c^2=-c$ , soit  $-bc=-c$  (cad  $bc=c$ ), soit  $(1-b)c=0$  et comme  $a+b=1$ , on obtient  $ac=0$ .

### Exercice 3

1)  $x=c$ ,  $y=b$  donnent  $x^2+y^2=0$ , avec  $x$  et  $y$  non nuls.

2) Supposons que  $x^2+y^2=0 \Leftrightarrow x^2=-y^2$ , avec  $x$  et  $y$  deux nombres décadiques non nuls.

Si  $y$  n'est pas diviseur de 0, alors il est inversible (voir chapitre 5) et  $(x/y)^2=-1$ , ce qui est impossible car  $-1$  n'a pas de racine carrée (voir P9.1).

Donc  $y$  est diviseur de 0, de même  $x$  est diviseur de 0.

$xy=0$  donne  $x^2y^2=0$ , puis  $y^4=0$ , donc  $y=0$  (voir 6 de P9.1), contraire à l'hypothèse. Donc  $x$  et  $y$  ne sont pas associés, et ainsi d'après P8.9, ce sont des diviseurs de 0 associés à un même 3ième.

On peut vérifier ce dernier aspect directement : soit  $z$  non nul tel que  $xz=0$ , alors  $x^2z^2=0$ , puis  $y^2z^2=0$  et  $yz=0$ .

### Exercice 4

Puisque  $x^5=x$  entraîne  $(x^2)^3=x^2$ , c'est que nécessairement  $x^2 \in S_3$ , cad  $x$  est une racine carrée d'un élément de  $S_3$  : il suffit donc de chercher les racines carrées des éléments de  $S_3$  et d'examiner celles qui sont effectivement solutions de  $x^5=x$ .

$$x^2=0 \Leftrightarrow x=0 \text{ (voir P9.1)}$$

$$x^2=-1 \text{ est impossible (voir P9.1)}$$

$$x^2=1 \Leftrightarrow x=-1 \text{ ou } 1 \text{ ou } a-b \text{ ou } b-a \text{ (voir P9.1)}$$

$$x^2=a \Leftrightarrow x=-a \text{ ou } a \text{ (voir P9.3)}$$

$$x^2=b \Leftrightarrow x=-b \text{ ou } b \text{ (voir P9.3)}$$

$$x^2=-a \text{ est impossible (voir P9.9)}$$

$$x^2=-b \Leftrightarrow x=-c \text{ ou } c \text{ (voir P9.3, cf } c^2=-b)$$

$$x^2=a-b \Leftrightarrow x=-a-c \text{ ou } -a+c \text{ ou } a-c \text{ ou } a+c, \text{ puisque ces quatre nombres (distincts) ont pour carrés } a^2+c^2=a-b, \text{ et on utilise P8.10}$$

$$x^2=b-a \text{ est impossible, car sinon } (a-b)(b-a) \text{ aurait des racines carrées, or } (a-b)(b-a)=-1 \text{ qui n'a pas de racine carrée.}$$

Donc l'équation  $x^5=x$  a au plus 15 solutions : 0,  $-1$ , 1,  $a-b$ ,  $b-a$ ,  $-a$ ,  $a$ ,  $-b$ ,  $b$ ,  $-c$ ,  $c$ ,  $-a-c$ ,  $-a+c$ ,  $a-c$ ,  $a+c$  (ces 15 nombres sont distincts, puisque ce sont les racines carrées (distinctes) de nombres distincts).

On les examine une à une pour voir lesquelles sont effectivement des solutions : en fait elles le sont toutes!

Remarquons que si  $x$  est solution,  $-x$  l'est aussi puisque 5 est impair.

pour 0,  $-1$ , 1,  $-a$ ,  $a$ ,  $-b$ ,  $b$  c'est évident

cf  $ab=0$ ,  $(a-b)^5=a^5-b^5=a-b$ , donc  $a-b$  solution, et  $b-a$  aussi

$c^3 = -c$ , donc  $c^5 = -c^3 = c$ , donc  $c$  est solution et  $-c$  aussi  
 cf  $ac=0$ ,  $(-a+c)^5 = (-a)^5 + c^5 = -a+c$ , donc  $-a+c$  est solution et  $a-c$  aussi  
 de même  $-a-c$  et  $a+c$  sont solutions

Donc on a bien  $S_5 = \{0 ; -1 ; 1 ; -a ; a ; -b ; b ; a-b ; b-a ; -c ; c ; -a-c ; -a+c ; a-c ; a+c\}$ .

L'ensemble des carrés de ces 15 solutions est évidemment  $\{0 ; 1 ; a ; -b ; b ; a-b\}$ , puisque ces 15 solutions ont été obtenues en tant que racines carrées de ces 7 nombres!

Cherchons maintenant les racines carrées de chaque solution de  $x^5 = x$ .  
 Vu ce qui a été fait ci-dessus, on a tout de suite

0 a pour racine carrée 0  
 -1 n'a pas de racine carrée  
 1 a pour racines carrées -1, 1,  $a-b$ ,  $b-a$   
 -a n'a pas de racine carrée  
 a a pour racines carrées -a, a  
 -b a pour racines carrées -c, c  
 b a pour racines carrées -b, b  
 $a-b$  a pour racines carrées  $-a+c$ ,  $-a-c$ ,  $a-c$ ,  $a+c$   
 $b-a$  n'a pas de racine carrée

Reste à examiner les six dernières solutions.

$c$  n'a pas de racine carrée, car il se termine par 2 (voir P9.7 ou P9.9)  
 $-c$  n'a pas de racine carrée, car il se termine par 8 (voir P9.7 ou P9.9)  
 et  $a$  se terminant par 5 et  $c$  par 2  
 $-a-c$  se termine par 3 et donc n'a pas de racine carrée (voir P9.7)  
 $-a+c$  se termine par 7 et donc n'a pas de racine carrée (voir P9.7)  
 $a-c$  se termine par 3 et donc n'a pas de racine carrée (voir P9.7)  
 $a+c$  se termine par 7 et donc n'a pas de racine carrée (voir P9.7)

Donc l'ensemble des racines carrées des éléments de  $S_5$  est exactement  $S_5$ .

### Exercice 5

$x^5 = -x$  entraîne  $(x^2)^3 = -x^2$ , donc  $x^2 \in S_{-,3} = \{0 ; -c ; c\}$ . Comme  $-c$  et  $c$  n'ont pas de racine carrée, la seule possibilité est  $x=0$ , qui bien sûr convient.

### Exercice 6

Il s'agit de généraliser la démonstration faite dans le cas  $p=1$  ( $x^2 = x$ ), lors de l'exercice du chapitre 6.

Cela se fait sans trop de difficulté sauf dans le cas où  $2p-1 \equiv 5 \pmod{10}$ , cas qui nécessite un raisonnement particulier assez longuet, mais il y a peut être mieux ... !

Le même raisonnement fait pour  $x^2 = x$  donne

**$x$  solution de  $x^{2p} = x \Leftrightarrow x$  est entier décadique et pour tout  $n \geq 0$ ,  $([x]_n)^{2p} \equiv [x]_n \pmod{10^{n+1}}$ . Cette congruence sera appelée la relation  $P_n$ .**

**On pose, pour  $n \in \mathbb{N}$ ,  $r_n = (([x]_n)^{2p} - [x]_n) / 10^{n+1}$  et  $w_{n+1}$  = le chiffre de rang  $n+1$  de  $([x]_n)^{2p}$   
 Si  $P_n$  est vraie, alors  $r_n \in \mathbb{N}$  et  $r_n \equiv w_{n+1} \pmod{10}$ .**



En effet,  $P_n$  vraie donne  $([x]_n)^{2p} = [x]_n + r_n 10^{n+1}$ , avec  $r_n$  dans  $\mathbb{N}$  ; donc  $w_{n+1}$  est le chiffre des unités de  $r_n$ , soit  $r_n \equiv w_{n+1} \pmod{10}$ .

Pour  $n \in \mathbb{N}^*$ ,  $P_n$  sera vérifiée si et seulement si  $(10^n x_n + [x]_{n-1})^{2p} \equiv 10^n x_n + [x]_{n-1} \pmod{10^{n+1}}$ , ce qui équivaut à  $10^n (2p([x]_{n-1})^{2p-1} - 1)x_n + ([x]_{n-1})^{2p} - [x]_{n-1} \equiv 0 \pmod{10^{n+1}}$ .

Cela exige que  $10^n$  divise  $([x]_{n-1})^{2p} - [x]_{n-1}$ , donc que  $P_{n-1}$  soit vraie, et alors  $([x]_{n-1})^{2p} - [x]_{n-1} = 10^n r_{n-1}$ , avec  $r_{n-1}$  entier naturel.

Donc  $x$  vérifie  $P_n \Rightarrow x$  vérifie  $P_{n-1}$  et  $(2p([x]_{n-1})^{2p-1} - 1)x_n + r_{n-1} \equiv 0 \pmod{10}$

Réciproquement, si on a ces deux conditions, en multipliant la 2ième par  $10^n$ , on voit que  $x$  vérifie  $P_n$ .

Donc  $x$  vérifie  $P_n \Leftrightarrow x$  vérifie  $P_{n-1}$  et  $(2p([x]_{n-1})^{2p-1} - 1)x_n + r_{n-1} \equiv 0 \pmod{10}$

Comme par ailleurs  $[x]_{n-1} \equiv x_0 \pmod{10}$

**Pour tout  $n$  dans  $\mathbb{N}^*$ ,  $x$  vérifie  $P_n \Leftrightarrow x$  vérifie  $P_{n-1}$  et  $(2px_0^{2p-1} - 1)x_n \equiv -r_{n-1} \pmod{10}$**

Enfin,  $P_{n-1}$  vérifiée entraînant  $r_{n-1} \equiv w_n \pmod{10}$ , on peut écrire aussi

**pour tout  $n$  dans  $\mathbb{N}^*$ ,  $x$  vérifie  $P_n \Leftrightarrow x$  vérifie  $P_{n-1}$  et  $(2px_0^{2p-1} - 1)x_n \equiv -w_n \pmod{10}$**

Donc, puisque  $x^{2p} = x \Rightarrow$  que pour tout  $n$  dans  $\mathbb{N}$ ,  $P_n$  est vraie, c'est que  $x^{2p} = x \Rightarrow P_0$  vraie et pour tout  $n$  dans  $\mathbb{N}^*$ ,  $(2px_0^{2p-1} - 1)x_n \equiv -w_n \pmod{10}$  ;

Réciproquement si on a  $P_0$  vraie et pour tout  $n$  dans  $\mathbb{N}^*$ ,  $(2px_0^{2p-1} - 1)x_n \equiv -w_n \pmod{10}$ , alors,  $P_0$  est vraie, et comme  $(2px_0^{2p-1} - 1)x_1 \equiv -w_1 \pmod{10}$ , c'est que  $P_1$  est vraie.

Et comme  $(2px_0^{2p-1} - 1)x_2 \equiv -w_2 \pmod{10}$ , c'est que  $P_2$  est vraie.

Etc : pour tout  $n$  dans  $\mathbb{N}$ , on a  $P_n$  vraie, donc  $x^{2p} = x$ .

**Finalement :  $x^{2p} = x \Leftrightarrow P_0$  vraie et pour tout  $n$  dans  $\mathbb{N}^*$ ,  $(2px_0^{2p-1} - 1)x_n \equiv -w_n \pmod{10}$**

$P_0$  vraie étant équivalent à  $(x_0)^{2p} \equiv x_0 \pmod{10}$ , **les seules possibilités pour  $x_0$  sont 0 ou 1 ou 5 ou 6.**

En effet :

pour 0 et 1, c'est évident

si  $x_0 = 5$  aussi, puisque toute puissance de 5 se termine par 5

si  $x_0 = 6$  aussi, puisque toute puissance de 6 se termine par 6

si  $x_0 = 2$  c'est impossible car  $2^k$  se termine par 2  $\Leftrightarrow k = 4k' + 1$ , avec  $k'$  dans  $\mathbb{N}$

Explication : modulo 10,  $2^0 \equiv 1$ ,  $2^1 \equiv 2$ ,  $2^2 \equiv 4$ ,  $2^3 \equiv 8$ ,  $2^4 \equiv 6$ ,  $2^5 \equiv 2$ , d'où le reste 2 n'apparaît que pour les puissances 1, 5, 9,...

On peut aussi écrire que pour tout  $k'$  dans  $\mathbb{N}^*$ ,  $2^{4k'} = (16)^{k'} \equiv 6^{k'} \equiv 6 \pmod{10}$  ; donc, toujours pour  $k'$  dans  $\mathbb{N}^*$ ,  $2^{4k'+1} \equiv 2 \pmod{10}$ ,  $2^{4k'+2} \equiv 4 \pmod{10}$ ,  $2^{4k'+3} \equiv 8 \pmod{10}$  ; mais ces trois dernières congruences sont aussi vraies pour  $k' = 0$ , alors que  $2^{4 \times 0} \equiv 1 \pmod{10}$ .

si  $x_0 = 3$  c'est impossible car  $3^k$  se termine par 3  $\Leftrightarrow k = 4k' + 1$ , avec  $k'$  dans  $\mathbb{N}$

si  $x_0 = 4$  c'est impossible car  $4^k$  se termine par 4  $\Leftrightarrow k = 2k' + 1$ , avec  $k'$  dans  $\mathbb{N}$

si  $x_0 = 7$  c'est impossible car  $7^k$  se termine par 7  $\Leftrightarrow k = 4k' + 1$ , avec  $k'$  dans  $\mathbb{N}$

si  $x_0 = 8$  c'est impossible car  $8^k$  se termine par 8  $\Leftrightarrow k = 4k' + 1$ , avec  $k'$  dans  $\mathbb{N}$

si  $x_0 = 9$  c'est impossible car  $9^k$  se termine par 9  $\Leftrightarrow k = 2k' + 1$ , avec  $k'$  dans  $\mathbb{N}$

D'où  **$x^{2p} = x \Leftrightarrow x_0 = 0$  ou 1 ou 5 ou 6 et pour tout  $n$  dans  $\mathbb{N}^*$ ,  $(2px_0^{2p-1} - 1)x_n \equiv -w_n \pmod{10}$**

On voit alors tout de suite que si  $2px_0^{2p-1} - 1$  est inversible modulo 10, alors pour tout  $n$  dans  $\mathbb{N}^*$ ,  $x_n$  existe et est unique, et donc il existe un et un seul  $x$  tel que  $x^{2p} = x$  dont le terme de rang 0 sera cet  $x_0$ .

Malheureusement, dans le cas  $x_0 = 1$  et  $2p - 1 \equiv 5 \pmod{10}$ ,  $2px_0^{2p-1} - 1$  n'est pas inversible modulo 10 : ce cas va être plus compliqué à traiter.

si  $x_0=0$ , alors  $2px_0^{2p-1}-1=-1$  et  $x_n \equiv w_n \pmod{10}$ , donc  $x_n$  existe et est unique : **il existe une seule solution se terminant par 0 : c'est 0**, puisque 0 est effectivement une solution se terminant par 0. On peut le vérifier :  $w_1=0$ , donc  $x_1=0$ , donc  $w_2=0$ , donc  $x_2=0$ , etc...

si  $x_0=5$ , alors  $2p5^{2p-1}-1 \equiv -1 \pmod{10}$  et  $x_n \equiv w_n \pmod{10}$ , donc  $x_n$  existe et est unique : **il existe une seule solution se terminant par 5 : c'est a**, puisque a est effectivement une solution qui se termine par 5.

Si  $x_0=1$ , alors  $2px_0^{2p-1}-1=2p-1$ , et là il y a une petite difficulté, car  $2p-1$  n'est pas forcément inversible modulo 10.

En fait si  $2p-1 \equiv 1$  ou  $3$  ou  $7$  ou  $9 \pmod{10}$ , il est inversible modulo 10 et si  $p'$  est son inverse on a  $x_n \equiv -p'w_n \pmod{10}$ , donc  $x_n$  existe et est unique : il existe alors une seule solution se terminant par 1. C'est 1, puisque 1 est effectivement une solution qui se termine par 1.

On peut le vérifier :  $w_1=0$ , donc  $x_1=0$ , donc  $w_2=0$ , donc  $x_2=0$ , etc...

Mais si  $2p-1 \equiv 5 \pmod{10}$  alors ce raisonnement ne tient plus. On doit avoir  **$5x_n \equiv -w_n \pmod{10}$ . Cela exige que 5 divise  $w_n$ , et alors  $x_n \equiv -w_n/5 \pmod{2}$**

Cependant, la conclusion précédente est encore vraie (voir la preuve à l'annexe située ci-dessous : c'est assez longuet! Si quelqu'un a mieux...).

Enfin, **il existe toujours une seule solution se terminant par 1 : c'est 1**,

si  $x_0=6$ , alors  $6^{2p-1} \equiv 6 \pmod{10}$ , car une puissance (non nulle) de 6 se termine toujours par 6, donc  $2p6^{2p-1}-1 \equiv 2p-1 \pmod{10}$  et on retombe sur le problème rencontré dans le cas  $x_0=1$ , lorsque  $2p-1 \equiv 5 \pmod{10}$ .

Mais ici, on peut conclure rapidement puisque l'on sait que l'équation  $x^{2p}=x$ , a une seule solution se terminant par 0 (c'est 0) et une seule se terminant par 1 (c'est 1).

Supposons que l'équation admette deux solutions s et s' se terminant par 6.

Alors, cf P11.0, as et as' sont aussi deux solutions ; mais elles se terminent par 0, donc  $as=as'=0$ . La formule du binôme donne alors  $(a+s)^{2p}=a^{2p}+s^{2p}$ , soit  $(a+s)^{2p}=a+s$ , et ainsi a+s est solution de l'équation ; de même a+s' est solution. Or a+s et a+s' se terminent par 1, donc  $a+s=a+s'$ , soit  $s=s'$ .

Ce qui veut dire que l'équation admet au plus une solution se terminant par 6 ; comme b est effectivement une solution se terminant par 6, c'est qu'**il existe une seule solution se terminant par 6, c'est b**.

**On a donc prouvé que l'équation  $x^{2p}=x$  a exactement quatre solutions : 0, 1, a, b.**

**Annexe** : preuve que si  $2p-1 \equiv 5 \pmod{10}$ , l'équation  $x^{2p}=x$  (avec p dans  $\mathbb{N}^*$ ) a une seule solution se terminant par 1, qui est 1.

**On cherche donc à montrer que si x est tel que  $x^{2p}=x$  avec  $x_0=1$  et  $2p-1=5(2k_1+1)$ ,  $k_1$  étant dans  $\mathbb{N}$ , alors nécessairement  $x=1$ .**

Rappelons que pour tout entier naturel n, on a posé  $r_n = (([x]_n)^{2p} - [x]_n) / 10^{n+1}$  et  $w_{n+1}$  = le chiffre de rang n+1 de  $([x]_n)^{2p}$  ; mais ici  $P_n$  est toujours vraie (car on a supposé qu'effectivement  $x^{2p}=x$ ) alors  $r_n$  est entier naturel et  $r_n \equiv w_{n+1} \pmod{10}$ .

**On a donc nécessairement, puisqu'en outre  $2p-1 \equiv 5 \pmod{10}$ , pour tout n dans  $\mathbb{N}^*$ ,  $5x_n \equiv -w_n \equiv -r_{n-1} \pmod{10}$ .**

**Un résultat intermédiaire qui va être très utile :**

**lorsque  $2p-1=5^u(2v+1)$ , avec u et v entiers naturels, on peut écrire, en posant  $u'=5^u$  :**

$$r_n = [x]_n (([x]_n)^u - 1) g_n / 10^{n+1},$$

$$\text{avec } g_n = ([x]_n)^{u \times 2v} + ([x]_n)^{u \times (2v-1)} + \dots + ([x]_n)^u + 1$$

Cela en appliquant l'identité (valable dans tout anneau)  $t^k - 1 = (t-1)(t^{k-1} + t^{k-2} + \dots + t + 1)$ ,

$$\text{avec } t = ([x]_n)^u \text{ et } k = 2v + 1.$$

Et puisque pour tout  $n \geq 0$  on a  $[x]_n \equiv x_0 = 1 \pmod{10}$ , c'est que  $g_n \equiv 2v + 1 \pmod{10}$ , et donc  $g_n$  est impair et est divisible par 5 si et seulement si 5 divise  $2v + 1$ .

Soit  $j$  un entier  $\geq 1$  quelconque, tel que si  $j \geq 2$  on a  $x_1 = x_2 = \dots = x_{j-1} = 0$ .

Alors, puisque  $[x]_{j-1} = 1$ , on a  $r_{j-1} = 0$ , donc  $5x_j \equiv 0 \pmod{10}$ , soit  $x_j \equiv 0 \pmod{2}$  et donc nécessairement  $x_j = 2x'_j$  avec  $x'_j \equiv 0$  ou 1 ou 2 ou 3 ou 4.

Montrons que si  $x'_j \neq 0$ , alors

**pour tout  $n \geq j + 1$ , on a le résultat  $R_{j,n}$  suivant :**

$$\text{il existe } x_n \text{ tel que } 5x_n \equiv -r_{n-1} \pmod{10}$$

$$\Leftrightarrow$$

$$2p - 1 = 5^{n-j+1}(2k_n + 1), \text{ avec } k_n \text{ dans } \mathbb{N}$$

et alors, pour toute valeur possible de  $x_n$  telle que  $5x_n \equiv -r_{n-1} \pmod{10}$ , on a

$$10^n x_n + \dots + 10^j x_j = 2^{n+1} 5^j z_n \text{ avec } z_n \text{ entier naturel non divisible par 5.}$$

Montrons le par récurrence (sur  $n$ ):

$R_{j,j+1}$  est vrai

en effet  $5x_{j+1} \equiv -r_j \pmod{10}$  exige que 5 divise  $r_j = [x]_j (([x]_j)^5 - 1) g_j / 10^{j+1}$ , avec  $g_j \equiv 2k_1 + 1 \pmod{10}$ .

Et  $([x]_j)^5 - 1 = (10^j x_j + 1)^5 - 1$ , et puisque  $x_j = 2x'_j$ , et en appliquant la formule du binôme,

$$([x]_j)^5 - 1 = 10^{j+1} x'_j + 10(10^j \times 2x'_j)^2 + \dots = 10^{j+1}(x'_j + 10K), \text{ avec } K \text{ dans } \mathbb{N}.$$

Ainsi  $r_j = [x]_j (x'_j + 10K) g_j$ . Comme  $[x]_j$  se termine par 1, il n'est pas divisible par 5 ; de même  $x'_j + 10K$  n'est pas divisible par 5 puisque  $x'_j = 1$  ou 2 ou 3 ou 4.

Donc **5 divise  $r_j$**   $\Leftrightarrow$  5 divise  $g_j \Leftrightarrow$  5 divise  $2k_1 + 1$  (puisque  $g_j \equiv 2k_1 + 1 \pmod{10}$ ),  $\Leftrightarrow$   **$2p - 1 = 5^2(2k_{j+1} + 1)$**

Cette condition étant remplie, on doit avoir  $x_{j+1} \equiv -[x]_j (x'_j + 10K)(g_j/5) \pmod{2}$  ; mais  $[x]_j$  est impair (car se termine par 1), ainsi que  $g_j/5$  (puisque  $g_j$  est impair).

Donc  $x_{j+1} \equiv -x'_j \equiv x'_j \pmod{2}$ , et donc  $x_{j+1} + x'_j = 2q$ , avec  $q$  dans  $\mathbb{N}$ .

On a alors  $10^{j+1} x_{j+1} + 10^j x_j = 2 \times 10^j (4x_{j+1} + x_{j+1} + x'_j) = 2^{j+2} 5^j z_{j+1}$ , avec  $z_{j+1} = 2x_{j+1} + q$ .

Enfin, comme  $2z_{j+1} = 5x_{j+1} + x'_j$  et que  $x'_j$  n'est pas divisible par 5,  $z_{j+1}$  n'est pas divisible par 5.

Donc, le résultat  $R_{j,n}$  est bien vrai pour  $n = j + 1$

Montrons maintenant que pour tout  $n \geq j + 1$ , si  $R_{j,n}$  est vrai, alors  $R_{j,n+1}$  est vrai.

On procède comme ci-dessus, mais il va y avoir un petit problème technique supplémentaire...

$5x_{n+1} \equiv -r_n \pmod{10}$  exige que 5 divise  $r_n$ .

Mais ici, on a  $2p - 1 = 5^{n-j+1}(2k_n + 1)$ , et ainsi  $r_n = [x]_n (([x]_n)^e - 1) g_n / 10^{n+1}$ , avec  $e = 5^{n-j+1}$  et  $g_n \equiv 2k_n + 1 \pmod{10}$ , et par hypothèse de récurrence,  $[x]_n = 2^{n+1} 5^j z_n + 1$ , avec  $z_n$  non divisible par 5.

Par application de la formule du binôme,  $([x]_n)^e - 1 = 5^{n-j+1} 2^{n+1} 5^j z_n + \sum_{k=2}^e C_k^e (2^{n+1} 5^j z_n)^k$

**Le coefficient de  $z_n$  est exactement  $2^{n+1} 5^{n+1} = 10^{n+1}$ .**

Montrons maintenant que pour tout  $k \geq 2$ ,  $t_k = C_k^e (2^{n+1} 5^j z_n)^k$  est un multiple de  $10^{n+2}$ .

**val(n) étant l'exposant de 5 dans la décomposition en nombres premiers d'un entier naturel n**, pour tout q dans  $\mathbb{N}^*$  et pour tout  $k \in \{1; 2; \dots; 5^q\}$  on a, en posant  $u=5^q$ , **val( $C_u^k$ )=q-val(k)**

preuve :

on a  $1 \times 2 \times \dots \times k \times C_u^k = u(u-1)\dots(u-(k-1))$ .

Pour i quelconque dans  $\{1; 2; \dots; 5^q-1\}$  on peut écrire  $i=5^j r$  avec  $r \geq 1$ , r non divisible par 5 et  $j \leq q-1$  (sinon  $i \geq 5^q$ ).

Donc  $5^j$  divise  $5^q-i$ ; mais  $5^{j+1}$  divise  $5^q$  (puisque  $j+1 \leq q$ ), et  $5^{j+1}$  ne divise pas i (puisque 5 ne divise pas r) et donc  $5^{j+1}$  ne divise pas  $5^q-i$  : la plus grande puissance de 5 qui divise  $5^q-i$  est donc  $5^j$ , c'est-à-dire **val( $5^q-i$ )=j=val(i)**.

D'où, puisque  $\text{val}(nn')=\text{val}(n)+\text{val}(n')$  et  $k \leq 5^q \Rightarrow k-1 \leq 5^q-1$  :

$\text{val}(1)+\text{val}(2)+\dots+\text{val}(k)+\text{val}(C_u^k)=\text{val}(5^q)+\text{val}(1)+\text{val}(2)+\dots+\text{val}(k-1)$ , soit  $\text{val}(C_u^k)=\text{val}(5^q)-\text{val}(k)=q-\text{val}(k)$ .

On peut alors en déduire que pour tout  $k \geq 2$ ,  $t_k=C_e^k(2^{n+1}5^j z_n)^k$  est un multiple de  $10^{n+2}$ . En effet :

$t_k$  est multiple de  $2^{n+2}$  car  $k(n+1) \geq n+2$  (puisque  $k \geq 2$ ),

et montrer que  $t_k$  est un multiple de  $5^{n+2}$  équivaut à montrer (puisque 5 ne divise pas  $z_n$ ) que  $\text{val}((C_e^k)+kj) \geq n+2 \Leftrightarrow n-j+1-\text{val}(k)+kj \geq n+2 \Leftrightarrow (k-1)j-1 \geq \text{val}(k)$ .

si  $\text{val}(k)=0$ , c'est vrai puisque  $k-1$  et  $j$  étant  $\geq 1$ , on a  $(k-1)j-1 \geq 0$

si  $\text{val}(k) \geq 1$ , on peut écrire  $k=5^{\text{val}(k)}r$ , avec  $r \geq 1$ .

Or pour tout  $m \geq 1$  on a  $5^m-1=(1+4)^m-1 \geq 1+4m-1 \geq 4m \geq m+1$ , et donc  $5^{\text{val}(k)}-1 \geq \text{val}(k)+1$ .

Comme  $r \geq 1$ ,  $5^{\text{val}(k)}r-1 \geq 5^{\text{val}(k)}-1 \geq \text{val}(k)+1$ , soit  $k-1 \geq \text{val}(k)+1$ .

Et enfin,  $j \geq 1$  donne  $j(k-1) \geq k-1 \geq \text{val}(k)+1$ , soit  $j(k-1)-1 \geq \text{val}(k)$ , et  $t_k$  est bien multiple de  $5^{n+2}$

Donc  $t_k=C_e^k(2^{n+1}5^j z_n)^k$ , pour  $k \geq 2$ , est toujours un multiple de  $2^{n+2}5^{n+2}=10^{n+2}$ .

Enfinement  **$([x]_n)^e-1=10^{n+1}z_n+10^{n+2}K$ , avec K dans  $\mathbb{N}$ .**

Ainsi  $r_n=[x]_n(z_n+10K)g_n$ . Comme  $[x]_n$  se termine par 1, il n'est pas divisible par 5; de même  $z_n+10K$  n'est pas divisible par 5 puisque  $z_n$  n'est pas divisible par 5, par hypothèse de récurrence.

Donc  $x_{n+1}$  devant vérifier  $5x_{n+1} \equiv -r_n \pmod{10}$ , **5 doit diviser  $r_n \Leftrightarrow 5$  divise  $g_n \Leftrightarrow 5$  divise**

**$2k_n+1$  (puisque  $g_n \equiv 2k_n+1 \pmod{10}$ ),  $\Leftrightarrow 2k_n+1=5(2k_{n+1}+1) \Leftrightarrow 2p-1=5^{n-j+1} \times 5(2k_{n+1}+1)=5^{n-j+2}(2k_{n+1}+1)$**

Cette condition étant remplie, on doit avoir  $x_{n+1} \equiv -[x]_n(z_n+10K)(g_n/5) \pmod{2}$ ; mais  $[x]_n$  est impair (car se termine par 1), ainsi que  $g_n/5$  (puisque  $g_n$  est impair).

Donc  $x_{n+1} \equiv -z_n \equiv z_n \pmod{2}$ , et donc  $x_{n+1}+z_n=2q$ , avec q dans  $\mathbb{N}$ .

On a alors  $10^{n+1}x_{n+1}+\dots+10^j x_j=10^{n+1}x_{n+1}+2^{n+1}5^j z_n=2^{n+1}5^j(5^{n+1-j}x_{n+1}+z_n)=2^{n+1}5^j$

$((5^{n+1-j}-1)x_{n+1}+2q)=2^{n+1}5^j \times 2z_{n+1}$ , avec  $z_{n+1}=\frac{(5^{n+1-j}-1)x_{n+1}+q}{2}$ , entier naturel, car  $5^{n+1-j}-1$  est pair.

**Enfinement  $10^{n+1}x_{n+1}+\dots+10^j x_j=2^{n+2}5^j z_{n+1}$ , avec  $z_{n+1}$  entier naturel non divisible par 5, car  $2z_{n+1}=5^{n+1-j}x_{n+1}+z_n$  et  $z_n$  n'est pas divisible par 5.**

Donc, le résultat  $R_{j,n+1}$  est bien vrai, sachant que  $R_{j,n}$  est vrai.

**Donc, x vérifiant que  $x^{2^p}=x$  avec  $x_0=1$ , pour tout  $j \geq 1$ , tel que si  $j \geq 2$  on a  $x_1=x_2=\dots=x_{j-1}=0$ , alors  $x_j=2x'_j$  et si  $x'_j \neq 0$ , alors pour tout  $n \geq j+1$ , le résultat  $R_{j,n}$  est vrai.**

On va maintenant pouvoir démontrer facilement le résultat annoncé, à savoir : si  $2p-1 \equiv 5 \pmod{10}$ , l'équation  $x^{2p}=x$  (avec  $p$  dans  $\mathbb{N}^*$ ) a une seule solution se terminant par 1, qui est 1.

En effet, soit  $x$  vérifiant  $x^{2p}=x$  avec  $x_0=1$  :

le résultat précédent donne pour  $j=1$  :

$x_1=2x'_1$ , et si  $x'_1 \neq 0$ , alors pour tout  $n \geq 2$   $R_{1,n}$  est vrai, donc pour tout  $n \geq 2$ , il existe  $k_n$  (entier naturel) tel que  $2p-1=5^n(2k_n+1)$ , ce qui est évidemment impossible, la valuation de  $2p-1$  étant finie.

Donc  $x'_1=0$  et obligatoirement  $x_1=0$ .

le résultat précédent donne pour  $j=2$ , puisque  $x_1=0$  :

$x_2=2x'_2$ , et si  $x'_2 \neq 0$ , alors pour tout  $n \geq 3$   $R_{2,n}$  est vrai, donc pour tout  $n \geq 3$ , il existe  $k_n$  (entier naturel) tel que  $2p-1=5^{n-1}(2k_n+1)$ , ce qui est évidemment impossible, la valuation de  $2p-1$  étant finie.

Donc  $x'_2=0$  et obligatoirement  $x_2=0$ .

etc

Donc  $x^{2p}=x$  avec  $x_0=1$  entraîne que nécessairement  $x_j=0$  pour tout  $j \geq 1$ , ce qui entraîne  $x=1$ .

Comme 1 est effectivement solution de  $x^{2p}=x$ , c'est la seule solution de cette équation qui se termine par 1.

### Exercice 7

$x^7=x \Rightarrow (x^2)^4=x^2$ , donc  $x^2 \in S_4=\{0 ; 1 ; a ; b\}$ , donc nécessairement

$x^2=0$ , ce qui donne  $x=0$

ou  $x^2=1$ , ce qui donne  $x=-1$  ou  $1$  ou  $a-b$  ou  $b-a$

ou  $x^2=a$ , ce qui donne  $x=-a$  ou  $a$

ou  $x^2=b$ , ce qui donne  $x=-b$  ou  $b$

Réciproquement, on vérifie que ces seules possibilités sont effectivement solutions de  $x^7=x$ .  
Donc  $S_7=\{0 ; -1 ; 1 ; -a ; a ; -b ; b ; a-b ; b-a\}$ .

### Exercice 8

Pour  $n$  pair on a déjà vu (voir P11.3) que  $S_n=S_2$  qui est bien inclu dans  $S_5$ .

Le problème est le cas  $n$  impair.

Montrons tout d'abord que, pour  $p \geq 2$ , si  $S_p \subset S_5$  alors  $S_{2p-1} \subset S_5$  ; **ce résultat sera appelé (R)**

Si  $x \in S_{2p-1}$  alors  $x^{2p-1}=x$ , donc  $(x^2)^p=x^2$  et  $x^2 \in S_p$ , qui est inclu dans  $S_5$  (d'après l'hypothèse), et donc  $x \in S_5$ , puisque  $S_5$  est stable par racine carrée, d'après P11.2.

Montrons maintenant, par récurrence, que pour tout entier naturel  $n \geq 2$ , on a  $S_n \subset S_5$ .

$S_2 \subset S_5$  est vrai

$n$  étant un entier naturel  $\geq 2$ , supposons que pour tout  $p$  tel que  $2 \leq p \leq n$  on ait  $S_p \subset S_5$ .

alors

soit  $n$  est impair et  $n+1$  est pair et d'après P11.3, on a  $S_{n+1} \subset S_5$

soit  $n$  est pair :  $n=2q$  avec  $1 \leq q < n$ , donc  $2 \leq q+1 \leq n$ , et par hypothèse de récurrence on a

alors  $S_{q+1} \subset S_5$ , et cf le résultat (R)  $S_{2(q+1)-1} \subset S_5$ , soit  $S_{n+1} \subset S_5$

ainsi pour tout  $p$  tel que  $2 \leq p \leq n+1$  on a  $S_p \subset S_5$ .

Donc, par récurrence, **on a prouvé que pour tout  $n \geq 2$  on a  $S_n \subset S_5$ .**

Déterminons maintenant exactement les  $S_n$  : pour cela il suffit, pour chaque élément de  $S_5$ , de voir à quelle condition sur  $n$  il est effectivement une solution de  $x^n=x$ .

0, 1, a, b sont toujours solutions de  $x^n=x$  (évident)

chacun des nombres -1, -a, -b est solution de  $x^n=x \Leftrightarrow n$  impair (évident)

chacun des nombres a-b et b-a est solution de  $x^n=x \Leftrightarrow n$  impair

car  $(a-b)^n=a^n+(-1)^n b^n=a+(-1)^n b=a-b$  pour  $n$  impair,  $=a+b=1 \neq a-b$  pour  $n$  pair

chacun des nombres -c et c est solution de  $x^n=x \Leftrightarrow n=4p+1$

en effet :  $c^2=-b$ , donc  $c^{2p}=(-1)^p b=-b$  ou b, nombres distincts de c

$c^{2p+1}=(-1)^p b c=(-1)^p c$  (voir P11.1), d'où si  $p$  est pair  $c^{2p+1}=c$ , et donc c est solution, ainsi que -c, mais si  $p$  est impair  $c^{2p+1}=-c \neq c$ , donc c n'est pas solution, ainsi que -c.

Donc chacun des nombres -c et c est solution  $\Leftrightarrow n=2p+1$  avec  $p$  pair, soit  $n=4p+1$

chacun des nombres -a-c, -a+c, a-c, a+c est solution de  $x^n=x \Leftrightarrow n=4p+1$

en effet, u et v étant égaux chacun à -1 ou 1, posons  $E=(ua+vc)^n=u^n a+v^n c^n$  (puisque  $ac=0$ )

si  $n$  est pair  $E=a+c^{2p}=a+(-1)^p b$  et alors  $E=ua+vc$  ne pourrait être possible que si  $a=ua$  (on multiplie par a des deux côtés), donc  $u=1$  (car a distinct de -a), et  $E=ua+vc$  donne  $(-1)^p b=vc$ , ce qui est impossible puisque b n'est ni c, ni -c

si  $n$  est impair  $E=ua+vc^{2p+1}$  et alors  $E=ua+vc$  est possible  $\Leftrightarrow c^{2p+1}=c \Leftrightarrow p$  est pair (cf ci-dessus)

Donc  $ua+vc$  est solution  $\Leftrightarrow n=2p+1$  avec  $p$  pair, soit  $n=4p+1$

Donc

si  $n=4p+1$ , cad  $n \equiv 1 \pmod{4}$ , alors tous les éléments de  $S_5$  sont solutions de  $x^n=x$ , et donc  $S_n=S_5$

si  $n$  impair mais pas de la forme  $4p+1$ , donc de la forme  $4p+3$ , cad  $n \equiv 3 \pmod{4}$ , alors

$S_n=S_5-\{-c ; c ; -a-c ; -a+c ; a-c ; a+c\}$

si  $n$  pair alors  $S_n=\{0 ; 1 ; a ; b\}$

### Exercice 9

$x^n=-x \Rightarrow x^{2n}=x^2 \Rightarrow x^2 \in S_n \subset S_5 \Rightarrow x \in S_5$ , puisque  $S_5$  est stable par racine carrée.

Là encore, pour déterminer exactement les  $S_{-n}$ , il suffit, pour chaque élément de  $S_5$ , de voir à quelle condition sur  $n$  il est effectivement une solution de  $x^n=-x$ .

1, a, b, a-b, b-a, -a-c, -a+c, a-c, a+c ne sont jamais solutions pour 1, a, b c'est évident

$(a-b)^n=a-b$  ou  $a+b=1$ , lesquels sont différents de  $-(a-b)$

$(b-a)^n=b-a$  ou  $b+a=1$ , lesquels sont différents de  $-(b-a)$

u et v étant égaux chacun à -1 ou 1, posons  $E=(ua+vc)^n=u^n a+v^n c^n$

si  $n$  est pair  $E=a+c^{2p}=a+(-1)^p b$  et alors  $E=-ua-vc$  ne pourrait être possible que si  $a=-ua$  (on multiplie par a des deux côtés), donc  $u=-1$  (car a distinct de -a), et  $E=-ua-vc$  donne  $(-1)^p b=-vc$ , ce qui est impossible puisque b n'est ni c, ni -c

si  $n$  est impair  $E=ua+vc^{2p+1}=ua+v(-1)^p c$  et alors  $E=-ua-vc$  entraîne (on multiplie par a des deux côtés)  $ua=-ua$ , ce qui est impossible

0 est toujours solution

chacun des nombres -1, -a, -b est solution  $\Leftrightarrow n$  est pair (évident)

chacun des nombres -c et c est solution  $\Leftrightarrow n=4p+3$

en effet :

$c^{2p}=(-1)^pb$ , toujours distinct de  $c$

$c^{2p+1}=(-1)^pc$  sera égal à  $-c \Leftrightarrow p$  impair, soit  $n=2(2p+1)+1=4p+3$

Ceci donne immédiatement le résultat annoncé dans P11.5 sur les  $S_{..n}$ .

### Exercice 10

$x^n=1 \Rightarrow x^{n+1}=x$ , et comme  $n+1 \geq 2$ ,  $x \in S_{n+1} \subset S_5$ , et donc **toute racine nième de 1 est dans  $S_5$**

Là encore, pour déterminer ces racines nièmes, il suffit, pour chaque élément de  $S_5$ , de voir à quelle condition sur  $n$  il est effectivement une solution de  $x^n=1$ .

0, a, b, -a, -b, c, -c ne sont jamais des racines nièmes de 1

pour les premiers de cette liste, c'est évident ; et  $c^{2p}=(-1)^pb$ ,  $c^{2p+1}=(-1)^pc$ , quantités qui ne sont jamais égales à 1

1 est toujours racine nième de 1

chacun des nombres -1, a-b, b-a est racine nième de 1  $\Leftrightarrow n \equiv 0$  ou 2 (4)

en effet,  $(a-b)^n = a + (-1)^nb$  qui sera égal à 1  $\Leftrightarrow n$  est pair  $\Leftrightarrow n \equiv 0$  ou 2 (4) ; idem pour b-a

chacun des nombres -a-c, -a+c, a-c, a+c est racine nième de 1  $\Leftrightarrow n \equiv 0$  (4)

en effet, u et v étant égaux chacun à -1 ou 1, posons  $E=(ua+vc)^n = u^na + v^nc^n$

si n est pair, soit  $n=2p$ , alors  $E=a+c^{2p}=a+(-1)^pb$  qui sera égal à 1  $\Leftrightarrow p$  est pair, soit  $p=2q$ , soit  $n=4q \Leftrightarrow n \equiv 0$  (4)

si n est impair, soit  $n=2p+1$ , alors  $E=ua+vc^{2p+1}=ua+v(-1)^pc$  et alors  $E=1$  entraîne (on multiplie par a des deux côtés)  $ua=a$ , donc  $u=1$  (car -a distinct de a) et  $E=1$  donne  $v(-1)^pc=b$ , ce qui est impossible, b n'étant pas -c ou c.

Ceci donne immédiatement le résultat annoncé dans P11.6.

Remarque :

on peut trouver "directement" les racines 4ièmes de 1.

En effet,  $x^4=1 \Rightarrow x^2 \in S_2$ , donc x est nécessairement une racine 2ième de -1 ou 1 ou a-b ou b-a.

Mais on a vu que -1 n'a pas de racine carrée ( voir remarque 3 de P9.4), b-a non plus (voir P11.2)

alors que -1 a pour racines carrées -1, 1, a-b, b-a (voir P9.1) et a-b a pour racines carrées -a-c, -a+c, a-c, a+c (voir P11.2) ; réciproquement ces huit nombres sont bien racines 4ièmes de 1, et ce sont les seules.

[retour début du chapitre 11](#)

[Retour vers le sommaire de la page sur les nombres décadiques](#)

