Extension de Q engendrée par la racine d'un nombre premier.

*Ce problème regroupe des résultats très classiques sur des structures algébriques « remarquables » de sous-ensembles « particuliers » de **R**.*

1. Le sujet

0. Soit p un nombre premier. Démontrer que le nombre $\sqrt{p}$ est un nombre irrationnel.

Partie A. Des sous-corps de R.

Soit p un nombre premier.
On désigne par E l'ensemble de tous les nombres réels u s'écrivant sous la forme $u = x + y\sqrt{p}$ où x et y sont des rationnels. On peut aussi le noter sous cette forme $E = \{u,\ u = x + y\sqrt{p},\ x \in \mathbf{Q},\ y \in \mathbf{Q}\}$. Cet ensemble contient $\mathbf{Q}$ et la racine carrée de p.

1. Soient $u = x + y\sqrt{p}$ et $u' == x' + y'\sqrt{p}$ deux éléments de E (où x, x', y, y' sont des rationnels, on ne le rappellera plus). Montrer que $u = u'$ si et seulement si $x = x'$ et $y = y'$.

2. Soient $u = x + y\sqrt{p}$ et $u' == x' + y'\sqrt{p}$ deux éléments de E. Montrer que $u' - u$ et $u.u'$ sont aussi deux éléments de E. Que peut-on en déduire pour la structure algébrique de l'ensemble E ?

3. À tout élément $u = x + y\sqrt{p}$ de E, on associe l'élément de E appelé le « conjugué » de u : $\bar{u} = x - y\sqrt{p}$. Vérifier que le nombre $u.\bar{u}$ est un rationnel non nul si et seulement si u est non nul.
Utiliser ce résultat pour montrer que tout élément u non nul de E admet dans E un inverse pour la multiplication. Que peut-on en déduire pour la structure algébrique de l'ensemble E ?

Partie B. Des sous-anneaux denses de R.

Dans cette question, on désigne par F le sous-ensemble de E constitué par tous les nombres réels u s'écrivant sous la forme $u = x + y\sqrt{p}$ où x et y sont des entiers relatifs. On peut aussi le noter sous cette forme $F = \{u,\ u = x + y\sqrt{p},\ x \in \mathbf{Z},\ y \in \mathbf{Z}\}$. Ce sous-ensemble contient **Z** et la racine carrée de p.

1. Montrer que F est un sous-anneau de E.

NB. *La recherche des éventuels éléments de F qui ont un inverse dans F amènerait à rechercher les solutions dans* ***ZxZ*** *de l'équation* $x^2 - p\,y^2 = \pm 1$ *que je ne propose pas ici.*
Par exemple, lorsque $p = 2$*, les nombres* $3 - 2\sqrt{2}$ *et* $3 + 2\sqrt{2}$ *sont inverses l'un de l'autre, comme* $7 - 5\sqrt{2}$ *et* $7 + 5\sqrt{2}$ *ou* $17 - 12\sqrt{2}$ *et* $17 + 12\sqrt{2}$ *. On va en trouver incidemment quelques autres plus exotiques dans* ***B.4.***

2. L'ensemble F^{*+} des éléments de F qui sont strictement positifs est un ensemble non vide et minoré par zéro. Cet ensemble possède donc une borne inférieure positive ou nulle b. On se propose de montrer que en fait, $b = 0$

2.1. Supposons d'abord que b soit strictement positive et n'appartienne pas à F. Montrer qu'alors il existe deux éléments de F u et v tels que $b < u < v < 2b$, puis montrer que cette existence est contradictoire avec la définition de b.

2.2. Supposons ensuite d'abord que b soit strictement positive et appartienne à F. Montrer qu'alors F n'est autre que l'ensemble b**Z**, et que cela est contradictoire avec l'irrationnalité de la racine carrée de p.

2.3. Conclure.

3. Montrer qu'une conséquence en est que l'ensemble F est dense dans **R**.

4. Proposer un programme qui, un nombre premier p et un réel ε étant donnés, détermine et fait afficher le nombre $a - b\sqrt{p}$ (a et b entiers strictement positifs) tel que $0 < a - b\sqrt{p} \le \varepsilon$ et que a soit le plus petit possible.
Applications : $p = 2$; $\varepsilon = 10^{-3}$; $p = 2$; $\varepsilon = 10^{-5}$; $p = 2027$; $\varepsilon = 10^{-4}$

2. Eléments de correction

Rien d'inédit ni d'insolite dans ce problème. On aura l'occasion de voir ou revoir des démonstrations très classiques qu'un candidat au CAPES se doit de connaître.

0. Supposons que $\sqrt{p}$ soit un nombre rationnel. Il existe alors deux entiers a et b premiers entre eux (ce dernier non nul) tels que : $\frac{a}{b}=\sqrt{p}$.

Alors : $a^2 = pb^2$. Puisque p divise le second membre, il divise le premier membre. Puisque p est un nombre premier, s'il divise le carré de a, alors il divise a lui-même. Il existe un entier c tel que : $a = pc$. La relation $a^2 = pb^2$ s'écrit : $p^2c^2 = pb^2$ et par conséquent : $pc^2 = b^2$. Le nombre premier p divise le carré de b, donc il divise b lui-même. Il en résulte que p est un diviseur commun de a et de b, ce qui est contradictoire avec l'hypothèse « a et b premiers entre eux ». L'hypothèse « $\sqrt{p}$ est un nombre rationnel » aboutissant à une contradiction, c'est son contraire, l'hypothèse « $\sqrt{p}$ est un nombre irrationnel », qui est à retenir.

Partie A. Des sous-ensembles de R.
Soit p un nombre premier.
On désigne par E l'ensemble de tous les nombres réels u s'écrivant sous la forme $u = x + y\sqrt{p}$ où x et y sont des rationnels. On peut aussi le noter sous cette forme $E = \{u,\ u = x + y\sqrt{p},\ x \in \mathbf{Q},\ y \in \mathbf{Q}\}$

1. Soient $u = x + y\sqrt{p}$ et $u' == x' + y'\sqrt{p}$ deux éléments de E .

$u'-u = (x'-x)+(y'-y)\sqrt{p}$

Si $(y'-y)$ est non nul : $u'-u = (y'-y)\left(\left(\frac{x'-x}{y'-y}\right)+\sqrt{p}\right)$. L'irrationnalité de $\sqrt{p}$ justifie que $\left(\frac{x'-x}{y'-y}\right)+\sqrt{p}$ est non nul quelles que soient les valeurs de x et de x' (autrement, $\sqrt{p}$ serait un rationnel).

Donc, $(y'-y)$ non nul implique que $u'-u$ est non nul.

Par contraposition $u'-u=0 \Rightarrow y'-y=0$ et dans ce cas, si $u'-u=0$ et $y'-y=0$ alors $x'-x = u'-u-(y'-y)\sqrt{p}=0$. Finalement : $u'-u=0 \Rightarrow \begin{cases} x'-x=0 \\ y'-y=0 \end{cases}$ autrement dit : $u'-u=0 \Rightarrow \begin{cases} x'=x \\ y'=y \end{cases}$

2. Notons d'abord que E contient **Q**, comme l'indique l'énoncé (E est non vide …).

Soient $u = x + y\sqrt{p}$ et $u' == x' + y'\sqrt{p}$ deux éléments de E.

$u'-u = (x'-x)+(y'-y)\sqrt{p}$ et $u.u' = (xx + pyy') + (xy' + yx')\sqrt{p}$.

Compte tenu des propriétés algébriques de l'ensemble **Q**, les différences $(x'-x);(y'-y)$ appartiennent à **Q** (c'est un groupe additif) et les cocktails $(xx+pyy');(xy'+yx')$ aussi (c'est un anneau).

La différence et le produit de deux éléments de E appartiennent à E. E est un sous-groupe additif stable pour la multiplication. La structure algébrique de l'ensemble E est celle d'un sous-anneau de **R.**

3. À tout élément $u = x + y\sqrt{p}$ de E, on associe l'élément de E appelé le « conjugué » de u : $\overline{u} = x - y\sqrt{p}$. Alors $u.\overline{u} = \left(x + y\sqrt{p}\right)\left(x - y\sqrt{p}\right) = x^2 - p\,y^2$.

Si $u = x + y\sqrt{p} = 0$, alors d'après le résultat de la question **1**, $x = y = 0$ et par suite $x^2 - p\,y^2 = 0$

Réciproquement, si $x^2 - p\,y^2 = 0$ alors $y = 0$: si ce n'était pas le cas, l'écriture $p = \dfrac{x^2}{y^2}$ serait légitime, et cela contredirait l'irrationnalité du nombre $\sqrt{p}$. Dès lors que $x^2 - p\,y^2 = 0$ et que $y = 0$, on obtient : $x^2 = 0$ et par suite $x = 0$ puis finalement $u = 0$.

D'où l'équivalence : $u = 0 \Leftrightarrow x^2 - p\,y^2 = 0$

Il en résulte que, lorsque u est non nul, $x^2 - p\,y^2 \neq 0$ et $u.\dfrac{\overline{u}}{x^2 - p\,y^2} = 1$.

L'élément $u = x + y\sqrt{p}$ de E, lorsqu'il est non nul, admet pour inverse $\dfrac{x}{x^2 - p\,y^2} - \dfrac{y}{x^2 - p\,y^2}\sqrt{p}$

Tout élément u non nul de E admet dans E un inverse pour la multiplication : E est un sous-anneau de **R** dans lequel tout élément non nul a un inverse pour la multiplication, E est un sous-corps de **R**.

Partie B.

On désigne par F le sous-ensemble de E constitué par tous les nombres réels u s'écrivant sous la forme $u = x + y\sqrt{p}$ où x et y sont des entiers relatifs. On peut aussi le noter sous cette forme $F = \left\{u,\ u = x + y\sqrt{p},\ x \in \mathbf{Z},\ y \in \mathbf{Z}\right\}$. Cet ensemble est non vide car il contient **Z**.

1.1. En reprenant les notations de la partie précédente :
Soient $u = x + y\sqrt{p}$ et $u' = x' + y'\sqrt{p}$ deux éléments de F.
$u' - u = (x' - x) + (y' - y)\sqrt{p}$ et $u.u' = (x\,x + p\,y\,y') + (x\,y' + y\,x')\sqrt{p}$.
Compte tenu des propriétés algébriques de l'ensemble **Z**, les différences $(x' - x)$; $(y' - y)$ appartiennent à **Z** (c'est un groupe additif) et les cocktails $(x\,x + p\,y\,y')$;$(x\,y' + y\,x')$ aussi (c'est un anneau).
La différence et le produit de deux éléments de F appartiennent à F. La structure algébrique de l'ensemble F est celle d'un sous-anneau de E (et donc un sous-anneau de **R** par la même occasion).

2. L'ensemble F^{*+} des éléments de F qui sont strictement positifs est un ensemble non vide (il contient les entiers strictement positifs) et minoré par zéro. Cet ensemble possède donc une borne inférieure positive ou nulle b.

2.1. Supposons que b soit strictement positive et n'appartienne pas à F.
Il existe alors un élément u de F tel que $b < u < 2b$, sinon la borne inférieure de F serait $2b$.
Il existe un deuxième élément v de F tel que $b < v < u < 2b$, sinon la borne inférieure de F serait u.
Puisque u et v appartiennent tous deux à F, et que F est un groupe additif, la différence $u - v$ appartient aussi à F. Or, $0 < u - v < b$. Il existerait dans F^{*+} un élément strictement positif qui est strictement plus petit que sa borne inférieure, ce qui serait contradictoire avec la notion de borne inférieure.
Cette hypothèse est à éliminer.

2.2. Si b est strictement positive et appartient à F, tous ses multiples aussi et F contient l'ensemble $b\mathbf{Z}$. Autrement dit, $F \supset b\mathbf{Z}$.

Réciproquement, soit u un élément non nul de F. Il existe un entier relatif n tel que $nb \le u < (n+1)u$
L'hypothèse d'une inégalité stricte $nb < u < (n+1)u$ est à rejeter, sinon l'élément $u - nb$ serait un élément strictement positif de F qui serait strictement inférieur à la borne inférieure b. Nécessairement : $u = nb$, ce qui montre que tout élément de F appartient à $b\mathbf{Z}$. Autrement dit, $F \subset b\mathbf{Z}$.

Ainsi : F=$b\mathbf{Z}$. Il existe de ce fait d'une part un entier relatif n tel que : $\sqrt{p} = nb$ et d'autre part un entier relatif non nul m tel que : $1 = mb$. Alors : $\sqrt{p} = \dfrac{nb}{mb} = \dfrac{n}{m}$. Ce qui est contradictoire avec l'irrationnalité de la racine de p.
Cette hypothèse est à éliminer.

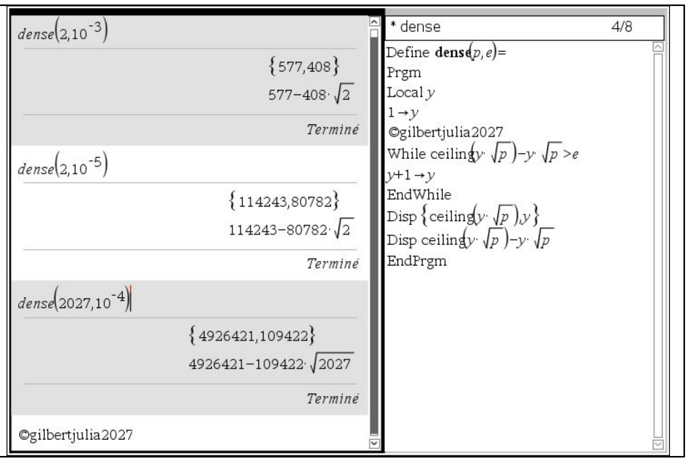
2.3. La seule hypothèse qui subsiste est : $b = 0$, puisque toutes les hypothèses où b est strictement positive ont été éliminées.

3. Soit x un nombre réel et ε un nombre réel strictement positif (aussi petit que l'on veut).

D'après **2.3**, il existe un élément u de F tel que $0 < u < \varepsilon$. Tout multiple entier de u est aussi dans F, et il existe un entier relatif n tel que : $nu \le x < (n+1)u$.
Alors : $0 \le x - nu < u < \varepsilon$, ce qui montre que $nu \in [x, x+\varepsilon[$. Quel que soit le réel x, et quel que soit le nombre réel strictement positif ε (aussi petit que l'on veut), il existe un élément de F dont la distance à x est plus petite que ε : F est dense dans **R**.

4. Proposer un programme qui, un nombre premier p et un réel ε étant donnés, détermine le nombre $a - b\sqrt{p}$ tel que $0 < a - b\sqrt{p} \le \varepsilon$ et que a soit l'entier le plus petit possible.
Applications : $p = 2$; $\varepsilon = 10^{-3}$; $p = 2$; $\varepsilon = 10^{-5}$; $p = 2027$; $\varepsilon = 10^{-4}$

4. Voici une proposition de programme avec TI-Nspire. On reconnaît entre autres les entiers 577 et 408 qui ont acquis une certaine « célébrité » car ils figurent dans le calcul d'une valeur approchée de la racine de 2 par la méthode de Héron lorsque la valeur initiale est 2.
(Avec $p = 2$ et $\varepsilon = 10^{-6}$, nous obtiendrions les entiers 665857 et 470832 qui sont successeurs de 577 et 408 dans l'algorithme de Héron).



Et la même chose, concordante (quel bonheur !), à l'aide de Python … Mais avec évidemment un peu plus de gaz tout frais sorti d'usine.

dense.py - C:\Users\Gilbert\Documents\dense.py (3.8.1)

File Edit Format Run Options Window Help

```python
from math import ceil,sqrt
p=int(input("Quel est le nombre premier p ?"))
e=float(input("Quel est le réel strictement positif epsilon ?
n=1
while ceil(n*sqrt(p))-n*sqrt(p)>e:
    n+=1
print(n)
print(ceil(n*sqrt(p)))
print(ceil(n*sqrt(p))-n*sqrt(p))
```

Python 3.8.1 Shell

File Edit Shell Debug Options Window Help

```
Python 3.8.1 (tags/v3.8.1:1b293b6, Dec 18 2019, 22:39:24) [MSC
tel)] on win32
Type "help", "copyright", "credits" or "license()" for more in
>>>
================= RESTART: C:\Users\Gilbert\Documents\dense.py
Quel est le nombre premier p ?2
Quel est le réel strictement positif epsilon ?0.001
408
577
0.0008665517772215026
>>>
>>>
================= RESTART: C:\Users\Gilbert\Documents\dense.py
Quel est le nombre premier p ?2
Quel est le réel strictement positif epsilon ?0.00001
80782
114243
4.376634024083614e-06
>>>
================= RESTART: C:\Users\Gilbert\Documents\dense.py
Quel est le nombre premier p ?2027
Quel est le réel strictement positif epsilon ?0.0001
109422
4926421
9.875372052192688e-05
>>>
```