1) (a) Donner la définition d'un idéal premier P dans un anneau commutatif R et la définition d'un anneau intègre.

(b) Soit R un anneau commutatif et soit $P \subsetneq R$. Montrer que

R/P est un anneau intègre $\Rightarrow$ P est un idéal premier

Solution : Soit R/P un anneau intègre. On sait déjà que $P \neq R$. Donc il reste à montrer que $rs \in P$ pour $r, s \in R$ implique que $r \in P$ ou $s \in P$. Mais $rs \in P$ veut dire que

$$(r+P)(s+P) = rs + P = P = 0_{R/P}$$

Donc soit $r+P = 0_P$, ie $r \in P$, soit $s+P = 0_P$, ie $s \in P$.

n'était pas demandé

Pour la réciproque on a que $R/P \neq 0$ car $P \neq R$. Soit $r+P = \bar{r}$ et $\bar{s} = s+P \in R/P$ tel que $\bar{r}\bar{s} = \bar{0} \in R/P$, ie $(r+P)(s+P) = rs + P = P$, ie $rs \in P$. Vu que P est un idéal premier, alors $r \in P$ ou $s \in P$. Mais ceci veut dire $s+P = \bar{r} = \bar{0}$ ou $\bar{s} = \bar{0}$.

2(a) Donner la définition d'un polynômes irréductible dans $F[x]$ où F est un corps.

Solution Un polynôme $p \in F[x]$ est irréductible si

(i) $\deg p \geq 1$ et

(ii) si $p = fg$ alors soit $f \in F$, soit $g \in F$

(b) Montrer que les polynômes suivantes sont irréductibles:

(i) $x^5 + 15x^2 + 30x + 5 \in \mathbb{Q}[x]$

(d'après Eisenstein avec $p=5$)

(ii) $x^3 + 7x^2 - 5 \in \mathbb{Q}[x]$

(Solution: $f = x^3 + 7x^2 - 5$ est irréductible ssi f n'a pas de racines dans $\mathbb{Q}$. D'après le critère sur les racines rationelles, ceci sont de diviseurs de 5, donc ± 5 et ± 1. Mais :

$f(5) = 125 + 175 - 5 = 295$, $f(-5) = -125 + 175 - 5 = 45$

$f(1) = 1 + 7 - 5 = 3$, $f(-1) = -1 + 7 - 5 = 1$)

(iii) $x^2 + x + 1 \in \mathbb{Z}_2[x]$

Solution f n'a pas de racines dans $\mathbb{Z}_2$ car

$f(1) = 1 = f(0)$.

2(c) Construire $GF(4)$, et son tableau de multiplication. Trouver un élément primitif dans $GF(4)$.

Solution On sait que $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ est irréductible, on sait que $\mathbb{Z}_2[x]/\langle f \rangle$ est un corps, donc un corps d'ordre 4. Alors, $GF(4) = \mathbb{Z}_2[x]/\langle f \rangle$. Soit $t = x + \langle f \rangle$. On a

$$t^2 = x^2 + \langle f \rangle = x+1 + \langle f \rangle = t + 1 \quad \text{dans } GF(4)$$

Donc $GF(4) = \{0, 1, t, t+1\}$ avec $t^2 = t+1$, et le tableau de la multiplication est

	0	1	t	$t+1$
0	0	0	0	0
1	0	1	t	$t+1$
t	0	t	$t+1$	1
$t+1$	0	$t+1$	1	t

On voit que $\langle t \rangle = \{t, t^2 = t+1, t^3 = t^2 + t = 1\} = GF(4) \setminus \{0\}$, donc t est un élément primitif.

2d) Soit $p \in F[x]$ où F est un corps. Prouver : Si $F[x]/\langle p \rangle$ est un corps, alors p est irréductible.

Solution On a $p \neq 0$ car $p = 0 \Rightarrow \langle p \rangle = 0$, $F[x]/\langle p \rangle = F[x]$ mais $F[x]$ n'est pas un corps car $F[x]^\times = F \setminus \{0\}$.

Aussi, $p \notin F \setminus \{0\}$ car $p \in F \setminus \{0\} = F[x]^\times$ implique $\langle p \rangle = F[x]$ donc $F[x]/\langle p \rangle = \{0\}$, contradiction car $0 \neq 1$ dans un corps. Alors, $\deg p \geq 1$.

Soit $p = fg$. Donc $0 = fg + \langle p \rangle = (f + \langle p \rangle)(g + \langle p \rangle)$. Alors, soit $f + \langle p \rangle = \langle p \rangle$, soit $g + \langle p \rangle = \langle p \rangle$. Supposons que $f + \langle p \rangle = \langle p \rangle$, c'est-à-dire $f \in \langle p \rangle$, par exemple $f = ph$, pour un $h \in F[x]$. Mais alors $p = (ph)g = p(hg)$, donc $hg = 1$ car $F[x]$ est un anneau intègre. Il s'ensuit que $g \in F[x]^\times = F \setminus \{0\}$, ie $g \in F$. De même manière : $g + \langle p \rangle = \langle p \rangle \Rightarrow f \in F$.

$(\sqrt{-5}$ au lieu $\sqrt{-1})$

3) Soit $R = \mathbb{Z}(\sqrt{-5}) = \{m+n\sqrt{-5} : m,n \in \mathbb{Z}\}$, un sous-anneau de $\mathbb{C}$.

(a) Déterminer $R^\times$

(b) Montrer que 2 est un élément irréductible dans R

(c) Est-ce que R est un anneau factoriel ? (Astuce: $2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

[3] Solution (a) Si $u = m+n\sqrt{-5}$ est inversible, alors $\frac{1}{m+n\sqrt{-5}} = \frac{m-n\sqrt{-5}}{m^2+5n^2} \in R$

Donc $m^2+5n^2 \mid m$. Alors $0 \le m^2+5n^2 \le |m|$. Si $m=0$, alors $n=0$ et $u=0$, $\lightning$! Donc $m \neq 0$, alors $m \le m^2$, donc $5n^2 = 0$, $n^2 = |m|$, i.e. $n=0$ et $m = \pm 1$. Alors, $R^\times = \{\pm 1\}$.

[6] (b) Un élément p est irréductible, si (1) $p \neq 0$ et $p \notin R^\times$, et (2) $p = ab \Rightarrow a \in R^\times$ ou $b \in R^\times$. Pour $p=2$ on a évidemment (1). Pour montrer (2), on utilise $N: R \to \mathbb{N}$, $N(m+n\sqrt{-5}) = m^2+5n^2 = |m+n\sqrt{-5}|^2$. On a $N(uv) = N(u)N(v)$. Alors, supposons que $2 = ab$. Donc $4 = N(2) = N(ab) = N(a)N(b)$. Il est clair que $R^\times = \{u \in R : N(u) = 1\}$. Donc, il suffit de montrer que $N(a) = 2$ est impossible : $2 = m^2+5n^2 \Rightarrow \lightning$! Donc $N(a) = 1$, ie $a \in R^\times$ ou $N(b) = 1$, ie $b \in R^\times$. Alors, 2 est irréductible.

[4] (c) R n'est pas factoriel, car dans un anneau factoriel chaque élément irréductible est premier. Supposons que 2 soit premier. De

$$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$$

découle que $2 \mid 1+\sqrt{-5}$ ou $2 \mid 1-\sqrt{-5}$. Supposons que $2 \mid 1+\sqrt{-5}$, i.e. $2a = 1+\sqrt{-5}$ pour un $a \in R$. Mais $1+5 = 6 = N(1+\sqrt{-5}) = N(2a) = N(2)N(a) = 4N(a)$ montre que $4 \mid 6$, $\lightning$! De même manière : $2 \nmid 1-\sqrt{-5}$. Alors, p n'est pas premier. Donc R n'est pas factoriel

4) Soit E/F une extension.

(a) Définir :

(i) $e \in E$ est un élément algébrique sur F

(ii) E/F est une extension algébrique

(c) Utiliser le Théorème de la multiplicativité de degrée des extensions pour prouver :

(i) Si $u_1, \dots u_n \in E$ sont algébrique sur F, alors $F(u_1, \dots, u_n)/F$ est une extension finie

(ii) Si D/F une sous-extension de E/F telle que D/F est une extension algébrique, alors chaque $e \in E$ qui est algébrique sur D l'est aussi sur F

(b) Prouver : Si E/F est une extension finie, alors E/F est une extension algébrique.

Preuve Soit $e \in E$ et soit $[E:F] = n+1 < \infty$. Alors, les éléments $1, e, \dots e^n$ sont linéairement dépendant. Donc, il y a $a_0, \dots a_n \in F$, pas tous $a_i = 0$, tels que $0 = a_0 + a_1 e + \dots + a_n e^n$, c'est-à-dire que $f(e) = 0$ pour $0 \neq f = a_0 + a_1 x + \dots + a_n x^n$.

Solution :

(a) Un élément $e \in E$ est algébrique sur F s'il y a $0 \neq f \in F[x]$ tel que $f(e) = 0$. On appelle E/F une extension algébrique si chaque $e \in E$ est algébrique sur F

(b) (i) Par induction sur n : Si $u \in E$ est algébrique, alors $F(u) = F[u]$ a un degré fini, car $F[u] = F[x]/\langle m_u \rangle$ Soit $n \geq 2$. On pose $D = F(u_1, \dots, u_{n-1})(u_n)$ et l'on observe que u_n est algébrique sur D. Alors, dans le tour

$F(u_1, \dots, u_n) = D(u_n)$ — les extensions $D(u_n)/D$ et D/F sont
D — des extensions finies, les dernières
F — d'après l'induction. Donc
$F(u_1, \dots, u_n)/F$ est une extension finie

(ii) Soit $f \in D[x]$ tq $f(e) = 0$. Disons $f = a_0 + a_1 x + \dots + a_n x^n$. Vu que $a_i \in D$, chaque a_i est algébrique sur F. Soit $C = F(a_0, \dots, a_n)$. D'après (i), C/F est une extension finie. Aussi e est algébrique sur C car $f \in C[x]$. Donc $C(e)/C$ est une extension finie. Alors, dans le tour des deux extensions $C(e)/C$ et C/F sont

$C(e)$ — de degrée fini, donc aussi $[C(e) : F] < \infty$.
C — Mais $F(e)/F$ est une sous-extension de $C(e)/F$,
F — donc aussi de degrée finie.

5. (a) Donnez la définition d'un corps de décomposition sur pour $f \in F[x]$, $\deg f \geq 1$ (F est un corps)

(b) Soit E un corps de décomposition pour $x^6 + x^3 - 2$ sur $\mathbb{Q}$. Trouver $[E : \mathbb{Q}]$ et une base de $E/\mathbb{Q}$

Solutions (a) Une extension E/F est un corps de décomposition pour $f \in F[x]$ si

(1) $f = a(x-u_1)\cdots(x-u_n)$, $u_i \in E$, $a \in F$, et

(2) $E = F(u_1, \ldots, u_n)$.

(b) En posant $y = x^3$ on a $f(x^3) = y^2 + y - 2 = (y-1)(y+2)$, donc $f(x) = (x^3-1)(x^3+2)$. Soit $w = e^{2\pi i/3} \in \mathbb{C}$. Alors, les racines de f sont $1, w, w^2$ (= racines de x^3-1), et $-\sqrt[3]{2}, -w\sqrt[3]{2}, -w^2\sqrt[3]{2}$ (les racines de x^3+2). Donc $E = \mathbb{Q}(\sqrt[3]{2}, w) = \mathbb{Q}(\sqrt[3]{2})(w)$. Vu que x^3+2 n'a pas de racines dans $\mathbb{Q}$, x^3+2 est irréductible sur $\mathbb{Q}$, donc $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. On peut factoriser $x^3 - 1 = (x-1)(x^2+x+1)$. Vu que $w \notin \mathbb{Q}(\sqrt[3]{2})$, x^2+x+1 est irréductible sur $\mathbb{Q}(\sqrt[3]{2})$. Alors $[E : \mathbb{Q}(\sqrt[3]{2})] = 2$ et $[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$.

Une base de $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ est $1, \sqrt[3]{2}, \sqrt[3]{4}$, et une base de $E/\mathbb{Q}(\sqrt[3]{2})$ est w, w^2. Donc, une base de $E/\mathbb{Q}$ est

$$w,\ w\sqrt[3]{2},\ w\sqrt[3]{4},\ w^2,\ w^2\sqrt[3]{2},\ w^2\sqrt[3]{4}.$$

[12] 6) Donner un exemple (sans preuve)

(1) d'un anneau non-commutatif, ($M_2(\mathbb{R})$)

(2) d'un anneau commutatif qui n'est pas un anneau intègre ($\mathbb{Z}_6$),

(3) d'un corps gauche, qui n'est pas un corps, (H)

(4) d'un homomorphisme $\mathbb{Z} \to \mathbb{Z}_6$ ($n \mapsto \overline{n}$)

(5) d'un polynôme irréductible dans $\mathbb{Q}[x]$ de degré n, $n \in \mathbb{N}$ arbitraire ($x^n - 2$, ou $x^n + x + 1$)

(6) d'un anneau factoriel, qui n'est pas un anneau principal ($\mathbb{Z}[x]$)

(7) d'un anneau Euclidien ($F[x]$, F corps, ou $\mathbb{Z}_{(p)}$)

(8) d'une extension algébrique $[E:F]$ telle que $[E:F] = \infty$, ($\mathbb{A}/\mathbb{Q}$, $\mathbb{A} = \{z \in \mathbb{C} : z \text{ algébrique sur } \mathbb{Q}\}$)

(9) d'un corps algébriquement clos, qui n'est pas $\mathbb{C}$, ($\mathbb{A}$)

(10) d'une extension transcendante, ($\mathbb{Q}(\pi)$)

(11) d'un polynôme irréductible dans $\mathbb{R}[x]$, deg $p \geq 2$. ($x^2 + 1$)

(12) d'un idéale premier dans $\mathbb{Z}$, qui n'est pas un idéal maximal : $\{0\}$

[5] 7) Soit A un anneau commutatif tel que l'intersection de tous ses idéaux premiers soit nulle. Montrer que A est isomorphe à un sous-anneau d'un produit de corps.

Solution: Pour chaque idéal premier P de A on note $\kappa(P)$ le corps de fractions de l'anneau intègre A/P, et l'on note φ_P l'homomorphisme canonique $\varphi_P : A \to \kappa(P)$, à savoir la composition

$$A \twoheadrightarrow A/P \hookrightarrow \kappa(P)$$

où $A \to A/P$ est l'épimorphisme canonique et $A/P \hookrightarrow \kappa(P)$ l'inclusion. Soit l'application

$$\varphi : A \to \prod_{\text{Pidéal premier}} \kappa(P)$$

dont la composante d'indice P est φ_P. Alors, φ est un homomorphisme et son noyau est

$$\ker(\varphi) = \bigcap_P \ker \varphi_P = \bigcap_P P = \{0\},$$

alors φ est injective.