TD n°4.

1 Anneaux factoriels

Exercice 1. Soit A un anneau intègre vérifiant la condition (E) d'existence d'une décomposition de tout élément en produit de facteurs irréductibles. Montrer l'équivalence des propositions suivantes :

a) A vérifie l'unicité de la décomposition (c'est-à-dire A est factoriel) ;

b) si p est irréductible, et p divise ab, alors p divise a ou b (lemme d'Euclide) ;

c) p est irréductible si et seulement si (p) est un idéal premier ;

d) si a divise bc et si a est premier avec b, alors a divise c (théorème de Gauss).

Solution. Commençons par remarquer que sans aucune hypothèse, on a que si (p) est premier, alors p est irréductible. En effet, si $p = ab$, alors on $ab \in (p)$, donc a ou $b \in (p)$ donc p divise a ou b.
L'équivalence de b) et c) est claire sans l'hypothèse que A vérifie (E). On a aussi (sans hypothèse (E)) : d) $\Rightarrow$ b) (car comme p est irréductible, si p ne divise pas a, alors p est premier avec a) et b) $\Rightarrow$ a) : en effet, si

$$a = t\prod p^{v_p(a)} = u\prod p^{w_p(a)},$$

on choisit p tel que $v_p(a) > 0$, comme p divise le second membre, il divise un de ses facteurs et on a $w_p(a) > 0$. On divise les deux membres par p et on recommence. On conclue par récurrence.
Il reste à prouver a) $\Rightarrow$ d) et on aura besoin de (E). On décompose a, b et c en facteurs irréductibles et il s'agit de montrer que $v_p(a) \leq v_p(c)$ pour tout p. Sinon, on a pour un p, $v_p(a) > v_p(c)$, or comme a divise bc, on a $v_p(b) \geq v_p(a) - v_p(c) > 0$ donc p divise a et b ce qui est impossible car ils sont premiers entre eux.

Exercice 2. Soit A un anneau factoriel et $a \in A$. Montrer que $\sqrt{aA}$ est un idéal principal.

Solution. Si $a = 0$, alors $\sqrt{(a)} = 0$ puisque A est intègre. Sinon, soit $a = \prod_i p_i^{n_i}$ la décomposition en facteurs irréductibles de a, avec $n_i \geq 1$. Soit $b = \prod_i p_i$. Alors $b^{\max_i n_i} \in (a)$ et donc $b \in \sqrt{(a)}$. Réciproquement si $c \in \sqrt{(a)}$, alors il existe n tel que a divise c^n. En particulier p_i divise c^n et donc p_i divise c d'après le lemme de Gauss. Donc $b = \prod_i p_i$divise c. Donc $\sqrt{(a)} = (b)$.

Exercice 3. Contenus
A désigne un anneau factoriel. On note $c(P)$ pour $P \in A[X]$, le contenu de P : c'est le pgcd de ses coefficients. P est primitif si $c(P)$ est inversible. On note $k = \mathrm{Frac}(A)[X]$.

a) Soit p premier un élément de A qui divise $P \cdot Q \in A[X]$. Montrer que p divise P ou Q. (Lemme de Gauss)

b) i) Montrer que, si P et Q sont primitifs, alors PQ est primitif
ii) Montrer que $c(P)c(Q) = c(PQ)$

c) Monrter que, si P primitif divise Q dans $k[X]$, alors P divise Q.

d) Montrer que $P \in A[X]$ est irréductible si et seulement si il est primitif et irréductible dans $k[X]$.

Solution. a) On a un morphisme $A \to A/(p)$ qui se prolonge en $A[X] \mapsto A/(p)[X]$, qui est intègre. Sinon, autre méthode. Supposons que p ne divise ni P, ni Q. Soit i_0 et j_0 les indices maximum tels que $p \not| p_i$ et $p \not| q_j$. Calculons $(PQ)_{i_0+j_0} = \sum_{i+j=i_0+j_0} p_i q_j$. Donc $p | p_{i_0} q_{j_0}$. Contradiction.

b) Tout diviseur premier de $c(PQ)$ divise $c(P)$ ou $c(Q)$ donc leur produit et réciproquement. ON fait une récurrence sur le nombre de facteurs dans la décomposition de $c(P)c(Q)$.

c) Soit $BP = Q$ où $B \in \mathrm{Frac(A)}[X]$. On peut multiplier pat d, tel que $dB \in A[X]$ et $c(dB) = 1$. On alors $(dB) \cdot P = dQ$. Mais $d | c(dQ) = c(dB)c(P) = 1$ donc d est inversible et $B \in A[X]$.

Exercice 4. Critère d'irréductibilité d'Eisenstein

a) soit A un anneau factoriel et K son corps des fractions. Soit $f = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynômes de degré $d \geq 1$. Soit p un élément irréductible de A. Supposons que p ne divise pas a_d, que p divise a_i pour $0 \leq i < d$ et que p^2 ne divise pas a_0. Montrer que f est irréductible dans $K[X]$.

b) Montrer que $X^4 + X^2Y^3 + Y$ est irréductible dans $\mathbb{Q}[X, Y]$.

c) Soient A est un anneau intègre et $\mathfrak{p}$ un idéal premier Soit $f = \sum_{i=0}^{d} a_i X^i \in A[X]$ un polynômes de degré $d \geq 1$ tel qu'aucun élément non inversible ne divise tous les coefficients. Supposons $a_d \notin \mathfrak{p}$, $a_i \in \mathfrak{p}$ pour $0 \leq i < d$ et que $a_0 \notin \mathfrak{p}^2$. Montrer que f est irréductible dans $A[X]$.

Solution. (i) Supposons que $f = PQ$ avec P et Q dans $K[X]$. On peut alors écrire $P(X) = \frac{1}{a}P_0(X)$ avec $P_0 \in A[X]$ et $a \in A$ tel qu'aucun facteur irréductible de a ne divise P_0. On écrit de même $Q(X) = \frac{1}{b}Q_0(X)$. On a alors $abf(X) = P_0(X)Q_0(X)$. Si p est un irréductible divisant ab, il divise P_0Q_0 donc d'après le lemme de Gauss, il divise P_0 ou Q_0. En le divisant on obtient une relation semblable avec un facteur irréductible de moins. On peut donc supposer par récurrence que ab est inversible puis en divisant encore que $a = b = 1$.
Remarquons tout d'abord que comme p est irréductible et que A est factoriel, alors l'idéal (p) est premier (cf. exercice précédent). On va donc se placer dans $A/(p)[X]$ qui est un anneau intègre. Avec les hypothèses, on peut alors calculer

$$Cl(a_d)X^d = Cl(f) = Cl(P)Cl(Q).$$

Il existe donc un entier k tel que $Cl(P) = Cl(\lambda)X^k$ et $Cl(Q) = Cl(\mu)X^{d-k}$ avec λ et $\mu \in A$ tels que $Cl(\lambda)Cl(\mu) = Cl(a_d)$. On sait alors que $\deg(P) \geq \deg(Cl(P)) = k$, $\deg(Q) \geq \deg(Cl(Q)) = d-k$ et $\deg(P)\deg(Q) = \deg(f) = d$. On en déduit que $\deg(P) = k$ et $\deg(Q) = d - k$. Si $k, d - k \geq 1$, alors $P(0)$ et $Q(0)$ sont divisibles par p, et donc $f(0)$ est divisible par p^2 contrairement à l'hypothèse. Donc P ou Q est de degré 0.
(ii) On se place dans $\mathbb{Q}[Y][X] = A[X]$ et on considère $p = Y$ qui est irréductible dans $A = \mathbb{Q}[Y]$. Le polynôme $X^4 + X^2Y^3 + Y$ vérifie les hypothèses du (i) donc il est irréductible dans $\mathbb{Q}(Y)[X]$ et donc à fortiori dans $\mathbb{Q}[X, Y]$.

Exercice 5. Soit A un anneau intègre et K son corps de fractions. On dit que $x \in K$ est entier sur A si $A[x]$ est un A-module de type fini. On dit que A est intégralement clos si tout élément de K entier sur A est dans A.

a) Montrer que $x \in K$ est entier sur A si et seulement si il existe un polynôme unitaire de $A[X]$ dont x est racine.

b) Montrer que si A est factoriel, alors A est intégralement clos.

Exercice 6. Montrer que $A = k[X, Y]/(X^2 - Y^3)$ est intègre et s'identifie à un sous-anneau de $k[T]$.

Solution. Il suffit de montrer que $X^2 - Y^3$ est irréductible dans $k[Y][X]$ et donc dans $k(Y)[X]$. Si $X^2 - Y^3$ est réductible, alors le polynôme à une racine dans $k(Y)$ (et même dans $k[Y]$ puisque $X^2 - Y^3$ est unitaire). D'où $P \in K[Y]$ tel que $P^2 = Y^3$. Alors $2\deg(P) = 3$, ce qui aboutit à une contradiction.
Soit $f : k[X, Y] \to k[T]$ l'unique morphisme d'anneau envoyant X sur T^3 et Y sur T^2. Alors $X^2 - Y^3 \in \ker(f)$, d'où par passage au quotient un morphisme d'anneau $\phi : A \to k[T]$. Comme $X^2 - Y^3$ est unitaire, la division euclidienne nous dit que A est un $k[Y]$-module libre de base $1, X$. Soit $P(Y)+XQ(Y) \in \ker\phi$, avec $P = \sum \alpha_i Y^i$ et $Q = \sum b_j Y^j$. Alors $\phi(P(Y)+XQ(Y) = \sum a_i T^{2i} + \sum b_i T^{2j+3} = 0$. Comme $2i \neq 2j+3$, la famille $(T^{2i})_i \cup T^{2j+3}$ est k-libre et donc $a_i = b_j = 0$. Donc ϕ est injective.

Exercice 7. Déterminer les décompositions en facteurs irréductibles de
(i) 120 dans le localisé $S^{-1}\mathbb{Z}$ avec $S = \{1, 2, 2^2, \cdots, 2^n, \cdots\}$.
(ii) 120 dans le localisé $S^{-1}\mathbb{Z}$ avec $S = \mathbb{Z} - (2)$, i.e. le localisé de $\mathbb{Z}$ en l'idéal premier (2).
(iii) $X^2Y^2 - X^3 - Y^3 + XY$ dans $\mathbb{C}[X, Y]$.
(iv) $-X^2Y + X^2Z + XY^2 - XZ^2 - Y^2Z + YZ^2$ dans $\mathbb{Q}[X, Y, Z]$.
(v) $X^n - Y$ dans $k[X, Y]$ où k est un corps.
(vi) $X^n + Y^n - 1$ dans $k[X, Y]$ où k est un corps.
(vii) $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ dans $k[a_0, \cdots, a_n, X]$ où k est un corps.

Solution. (i) On commence par écrire la décomposition en facteurs premiers de 120 dans $\mathbb{Z}$:

$$120 = 2^3 \times 3 \times 5.$$

Mais alors dans $S^{-1}\mathbb{Z}$, l'élément 2 devient inversible alors que les éléments 3 et 5 restent irréductibles (on a $S^{-1}\mathbb{Z}/3S^{-1}\mathbb{Z} = \mathbb{Z}/3\mathbb{Z}$ et $S^{-1}\mathbb{Z}/5S^{-1}\mathbb{Z} = \mathbb{Z}/5\mathbb{Z}$ qui sont des corps). Ainsi on a

$$120 \diamond 15 = 3 \times 5.$$

(ii) Dans ce cas ce sont 3 et 5 qui deviennent inversibles alors que 2 reste irréductible (on a $S^{-1}\mathbb{Z}/2S^{-1}\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$ qui est un corps). Ainsi on a

$$120 \diamond 8 = 2^3.$$

(iii) On peut écrire

$$X^2Y^2 - X^3 - Y^3 + XY = (X^2 - Y)(Y^2 - X).$$

Par ailleurs on voit que $\mathbb{C}[X,Y]/(X^2-Y)$ et $\mathbb{C}[X,Y]/(Y^2-X)$ sont isomorphes (échanger X et Y) et on a vu à l'exercice 26 qu'ils sont principaux et donc intègres (en fait ils sont isomorphes respectivement à $\mathbb{C}[X]$ et $\mathbb{C}[Y]$). Ainsi les idéaux (X^2-Y) et (Y^2-X) sont premiers et les éléments X^2-Y et Y^2-X sont irréductibles. L'écriture précédente était donc la décomposition en facteurs irréductibles.
(iv) On peut écrire

$$-X^2Y + X^2Z + XY^2 - XZ^2 - Y^2Z + YZ^2 = (X-Y)(Y-Z)(Z-X).$$

Par ailleurs on voit que $\mathbb{C}[X,Y,Z]/(X-Y)$, $\mathbb{C}[X,Y,Z]/(Y-Z)$ et $\mathbb{C}[X,Y,Z]/(Z-X)$ sont isomorphes (échanger X, Y et Z) et ils sont isomorphes respectivement à $\mathbb{C}[X,Z]$, $\mathbb{C}[X,Y]$ et $\mathbb{C}[Y,Z]$. Ils sont donc intègres. Ainsi les idéaux $(X-Y)$, $(Y-Z)$ et $(Z-X)$ sont premiers et les éléments $X-Y$, $Y-Z$ et $Z-X$ sont irréductibles. L'écriture précédente était donc la décomposition en facteurs irréductibles.
(v) Soit $A = k[X]$, $Y - X^n$ est un polynôme unitaire de degré 1, donc irréductible.
(vi) Soit $A = k[Y]$, l'élément $p = Y - 1$ est irréductible car $k[Y]/(Y-1) \simeq k$. Par ailleurs $Y-1$ divise $Y^n - 1$. Ainsi si $(Y-1)^2$ ne divise pas $Y^n - 1$, alors on est dans les hypothèses du critère d'Eisenstein.
Cependant, $(Y-1)^2$ divise $Y^n - 1$ si et seulement si $Y - 1$ divise le polynôme

$$\frac{\partial}{\partial Y}(Y^n - 1) = nY^{n-1}.$$

Ceci est équivalent à dire que $n = 0$ ce qui n'arrive que si la caractéristique du corps k divise n. Ainsi, si $\mathrm{car}(k) \not| \, n$, alors $X^n + Y^n - 1$ est irréductible.
Supposons maintenant que $p = \mathrm{car}(k) \,|\, n$. On écrit alors $n = p^a m$ avec $p \not| \, m$. On a alors

$$X^n + Y^n - 1 = (X^m)^{p^a} + (Y^m)^{p^a} - 1^{p^a}$$

mais d'après l'exercice 39, pour tout u et v en caractéristique p, on a $u^p + v^p = (u+v)^p$ et $u^p - v^p = (u-v)^p$. Ainsi, on voit que

$$(X^m)^{p^a} + (Y^m)^{p^a} - (1^m)^{p^a} = (X^m)^{p^a} + (Y^m - 1)^{p^a} = (X^m + Y^m - 1)^{p^a}.$$

Cependant comme $p \not| \, m$, on sait que $X^m + Y^m - 1$ est irréductible. Ainsi si $p = \mathrm{car}(k) \,|\, n$, avec $n = p^a m$, $p \not| \, m$, alors on a la décomposition en irréductibles

$$X^n + Y^n - 1 = (X^m + Y^m - 1)^{p^a}.$$

(vii) Dans $k[a_1, \cdots, a_n, X][a_0]$, $a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ est un polynôme unitaire de degré 1

Exercice 8. Montrer que le polynôme $X_1^2 + \cdots + X_n^2$ est irréductible pour $n \geq 2$ dans $\mathbb{R}[X_1, \cdots, X_n]$ et pour $n \geq 3$ dans $\mathbb{C}[X_1, \cdots, X_n]$.

Solution. Remarquons tout d'abord que si $n = 1$, alors X_1^2 n'est jamais irréductible. Ensuite, si $n = 2$ et qu'on se place sur le corps des nombres complexes, alors

$$X_1^2 + X_2^2 = (X_1 + \mathrm{i}X_2)(X_1 - \mathrm{i}X_2)$$

qui n'est donc pas irréductible. Il reste à montrer que dans les autres cas c'est irréductible. Voici deux méthodes.
Première méthode : supposons qu'il existe P et Q de degrés non nuls tels que $X_1^2 + \cdots + X_n^2 = PQ$. Alors on voit que P et Q sont de degrés 1. On écrit alors $P = \sum_i p_i X_i$ et $Q = \sum_i q_i X_i$. On a alors

$$PQ = \sum_{i=1}^{n} p_i q_i X_i^2 + 2\sum_{i<j}(p_i q_j + p_j q_i) X_i X_j.$$

On a donc $p_i q_i = 1$ (donc tous les p_i et les q_i sont inversibles) et $p_i q_j + p_j q_i = 0$. La dernière égalité nous donne

$$\frac{p_i}{q_i} = -\frac{p_j}{q_j}.$$

Supposons $n \geq 3$, alors on a

$$\frac{p_1}{q_1} = -\frac{p_2}{q_2},\ \frac{p_1}{q_1} = -\frac{p_3}{q_3} \text{ et } \frac{p_2}{q_2} = -\frac{p_3}{q_3}$$

ce qui donne

$$\frac{p_3}{q_3} = -\frac{p_3}{q_3}$$

c'est absurde.
Si les p_i et les q_i sont réels et que $n = 2$, alors on a $p_1q_1 = 1$, $p_2q_2 = 1$ et $p_1q_2 + p_2q_1 = 0$. En multipliant la dernière équation par p_1p_2, on obtient $p_1^2 + p_2^2 = 0$ ce qui impose $p_1 = p_2 = 0$ ce qui est impossible.
Deuxième méthode : on commence de la même manière : supposons qu'il existe P et Q de degrés non nuls tels que $X_1^2 + \cdots + X_n^2 = PQ$. Alors on voit que P et Q sont de degrés 1. On considère pour un polynôme P, l'ensemble

$$V(P) = \{(x_1, \cdots, x_n) \in k^n \ / \ P(x_1, \cdots, x_n) = 0\}.$$

Dans le cas des nombres réels, l'ensemble $V(X_1^2 + \cdots + X_n^2)$ est réduit au singleton $\{(0, \cdots, 0)\}$. Or l'ensemble $V(PQ) = V(P) \cup V(Q)$ est la réunion de deux hyperplans (puisque P et Q sont de degré 1). Mais alors si $n \geq 2$, cette réunion contient une infinité de points et ne peut donc être réduite au singleton $\{(0, \cdots, 0)\}$.
Dans le cas des nombres complexes, l'ensemble $V(Q)$ n'est plus un singleton et on ne peut raisonner de la même façon. Supposons $n \geq 3$. Alors $V(P) \cap V(Q)$ est l'intersection de deux hyperplans, elle est donc non réduite au singleton $(0, \cdots, 0)$. Soit $(x_1, \cdots, x_n) \in V(P) \cap V(Q)$ non nul. Il existe donc i tel que $x_i \neq 0$. On calcule

$$\frac{\partial(X_1^2 + \cdots + X_n^2)}{\partial X_i}(x_1, \cdots, x_n) = 2x_i.$$

Mais on a

$$\frac{\partial PQ}{\partial X_i}(x_1, \cdots, x_n) = \frac{\partial P}{\partial X_i}(x_1, \cdots, x_n)Q(x_1, \cdots, x_n) + P(x_1, \cdots, x_n)\frac{\partial Q}{\partial X_i}(x_1, \cdots, x_n) = 0.$$

On obtient $2x_i = 0$ alors que $x_i \neq 0$, c'est absurde.

Solution. Soit $a \in A$, comme A est factoriel, on dispose d'une décomposition en facteurs irréductibles :

$$a = u \prod_{i=1}^{r} p_i^{\alpha_i}$$

où u est inversible et les p_i sont irréductibles. Posons

$$a_{\text{red}} = \prod_{i=1}^{r} p_i,$$

nous allons montrer que $(A/(a))_{\text{red}} = A/(a_{\text{red}})$.
On commence par constater que comme $a_{\text{red}}|a$, alors $(a) \subset (a_{\text{red}})$ et donc $(a_{\text{red}})/(a)$ est un idéal de $A/(a)$. Par ailleurs, si $n = \max_i(\alpha_i)$, alors $a|a_{\text{red}}^n$ donc $Cl(a_{\text{red}})$ est nilpotent dans $A/(a)$ ainsi $(a_{\text{red}})/(a)$ est formé d'éléments nilpotents ou encore $(a_{\text{red}})/(a) \subset \text{nil(A/(a))}$.
Il reste donc à prouver que tout élément nilpotent $Cl(x) \in A/(a)$ est dans l'idéal $(a_{\text{red}})/(a)$. Pour un tel $Cl(x) \in \text{nil(A/(a))}$, il existe $n \in \mathbb{N}$ tel que $Cl(x)^n = 0$ c'est-à-dire $a|x^n$. Ainsi pour tout facteur irréductible p_i de a, on a $p_i|x^n$ et comme p_i est irréductible, $p_i|x$. Ceci impose que $a_{\text{red}}|x$ et donc $x \in (a_{\text{red}})$. On a donc $\text{nil(A/(a))} \subset \text{(a}_{\text{red}}\text{)/(a)}$ et donc

$$(A/(a))_{\text{red}} = A/(a_{\text{red}}).$$

Dans le cas $A = \mathbb{Z}$, on retrouve le résultat de l'exercice 4 (ɯ) : l'anneau $\mathbb{Z}/n\mathbb{Z}$ est réduit si et seulement si n n'a pas de facteur carré. Si n a des facteurs carrés, l'anneau $(\mathbb{Z}/n\mathbb{Z})_{\text{red}}$ est donc $\mathbb{Z}/(n_{\text{red}}\mathbb{Z})$.

Exercice 9. Soit $P = a_nX^n + \cdots + a_0$ un élément de $\mathbb{Z}[X]$. Et soit $r = \frac{p}{q} \in \mathbb{Q}$ une racine de P

a) $qX - p$ divise P.

b) i) En déduire que $p|a_0$

ii) En déduire que $q|a_n$

iii) En déduire que $p - q|P(1)$

iv) En déduire que $p + q|P(-1)$.

c) Trouver les racines rationelles de $A(x) = x^3 - 6x^2 + 15x - 14$ et $B(x) = x^4 - 2x^3 - 8x^2 + 13x - 24$.

Solution. a) Dans $\mathbb{Q}[X]$, on $X - p/q|P$, donc $qX - p$ divise P dans $\mathbb{Q}[X]$. $c(qX - p) = 1$ donc $qX - p$ divise P dans $\mathbb{Z}[X]$. On a donc $P = (qX - p)Q$.

b) i) On déduit de $P(0) = -pQ(0)$.

ii) On a $a_n = qq_{n-1}$.

iii) On a $P(1) = (q-p)Q(1)$

iv) On a $P(-1) = -(p+q)Q(-1)$.

c) Racines de $x^3-6x^2+15x-14$. On trouve que $p|14$, $q|1$, $p+q|36$, $p-q|4$. Les conditions restent inchangées par la transformation $(p,q) \mapsto (-p,-q)$. On a donc $q=1$, $p \in \{-1,0,1,2,3,5\} \cap \{-7,-2,-1,1,2,7\} = \{1,2\}$. On trouve $p=2, q=1$.
Racines de $x^4-2x^3-8x^2+13x-24$. On trouve $q=1$, $p|24$, $p+1|42$, $p-1|20$. On obtient $p=-3$.

Exercice 10. Soit n un entier premier à 10. Montrer que la suite des nombres 1, 11, 111, 1111, ... contient une infinité de multiples de n. Est-ce encore vrai pour la suite 17, 1717, 171717, ... ?

Solution.

Exercice 11. Trouver le pgcd et les coefficients de Bézout correspondants de $n-1$ et $n+1$ ainsi que ceux de n^2+1 et n^3-n.

Solution.

Exercice 12. Résolution de $3^m - 2^n = 1$

a) En raisonnant modulo 4, montrer que m est pair ou vaut 1.

b) si $m \neq 1$, $3^{m/2}-1$ et $3^{m/2}+1$ sont des puissances de 2.

c) Trouver les solutions de $3^m - 2^n = 1$.

Solution. a) Si $n=0$, il n'y a pas de solution à $3^m = 2$. Si $n=1$, $m=1$ est solution. Si $n \geq 2$ alors $2^n = 0 \mod 4$ et donc $3^m = (-1)^m = 1 \mod 4$, donc m est pair.

b) Si m est pair alors $2^n = 3^m - 1 = (3^{m/2}-1)\cdot(3^{m/2}+1)$. Par unicité de la décomposition, on a $3^{m/2}-1 = 2^k$ et $3^{m/2}+1 = 2^l$.

c) On a $2^l - 2^k = 2$ donc $2^k(2^{l-k}-1) = 2$ et donc $k=1$ et $l-k=1$. Soit $k=1$, $l=2$ et $n=k+l=3$. On trouve $n=3, m=2$.

Exercice 13. À quelle condition X^m+1 divise X^n+1 ?

a) Déterminer le PGCD de X^7-a et X^5-b.

b) si $a^5 = b^7$, X^7-a et X^5-b ont une racine commune. La déterminer.

c) Soit $P = X^2+1$ et $Q = X^3+1$. Déterminer le PGCD de P et Q. Quels sont les polynômes U et V vérifiant $UP+VQ = 1$?

Solution. On a, si $n > m$, $X^n+1 = (X^m+1)X^{n-m} + (1-X^{n-m})$. Donc X^m+1 divise X^n+1 si X^m+1 divise $X^{n-m}-1$. Si $n < 2m$, alors X^m+1 ne divise pas X^n+1. Sinon $X^{n-m}-1 = (X^m+1)X^{n-2m} + (X^{n-2m}+1)$. Si $n = mq+r$, on a donc $X^n+1 = X^r + (-1)^q \mod X^m+1$. On déduit que X^m+1 divise X^n+1 si et seulement si $n = (2k+1)m$.

a) On a $X^7-a = (X^5-b)X^2 + bX^2 - a$. Si $a=b=0$ alors $(X^7-a, X^5-b) = X^5$. Si $b=0$ et $a \neq 0$, alors $(X^7-a, X^5-b) = 1$. Sinon $(X^7-a, X^5-b) = (X^5-b, X^2-a/b)$. Mais $X^5-b = (X^2-b/a)(X^3+a/bX) + a^2/b^2X - b$. Si $a=0$ alors le pgcd vaut 1. Sinon $X^2-b/a = (X-b^3/a^2)(X+b^3/a^2) + (b^7-a^5)/a^4b$. On en déduit que si $a^5 \neq b^7$ le pgcd vaut 1, sinon, il vaut $X-b^3/a^2$.

b) La racine commune avut alors b^3/a^2.

c) On trouve $(1/2 - 1/2X - 1/2X^2)(X^2+1) + (1/2 + X/2)(X^3+1) = 1$.

Exercice 14. a) Trouver un pgcd de X^6-1 et de X^4-1 dans $\mathbb{C}[X]$, par factorisation et par l'algorithme d'Euclide.

b) Résoudre dans $\mathbb{C}[X]^2$, l'équation $P(X)(X^6-1) + Q(X)(X^4-1) = X^3+2X^2-X-2$.

c) Résoudre la même équation dans $\mathbb{R}[X]$.

Solution.

Exercice 15. Factorisations et congruences

a) Soit $P(X) = X^4+1$. Décomposer P dans $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ en produits de facteurs irréductibles.

b) Montrer que $-1, 2$ ou -2 est un carré dans $\mathbb{F}_p$ pour tout p.

c) Montrer que X^4+1 est factorisable dans $\mathbb{F}_p$ (on utilisera les égalités $X^4+1=(X^2+1)^2-2X^2=(X^2-1)^2+2X^2=(X^2)^2-(-1)$).

d) Factoriser $Q(X)=X^5-X-1$ dans $\mathbb{F}_5[X]$ (on vérifiera que si x est un élément d'une extension de degré 2 de $\mathbb{F}_5$, alors $x^{25}=x$) et en déduire que X^5-X-1 est irréductible dans $\mathbb{Q}[X]$.

e) Montrer que X^5-X^2-1 est irréductibles dans $\mathbb{Q}[X]$.

Solution. On a $X^4+1=(X^2+i)(X^2-i)=(X+\frac{1+i}{\sqrt{2}})(X-\frac{1+i}{\sqrt{2}})(X+\frac{1-i}{\sqrt{2}})(X-\frac{1-i}{\sqrt{2}})$.
On a $X^4+1=(X^2+1)^2-2X^2=(X^2-\sqrt{2}X+1)(X^2+\sqrt{2}X+1)$.
Si X^4+1 n'était pas irréductible dans $\mathbb{Q}[X]$, alors ce serait aussi une factorisation dans $\mathbb{R}[X]$. Or l'unique factorisation non triviale dans $\mathbb{R}[X]$ n'est pas rationelle. Donc X^4+1 est irréductible dans $\mathbb{Q}[X]$.
Puisque X^4+1 est unitaire, il est aussi irréductible dans $\mathbb{Z}[X]$.

a) Si $p=2$, -1 est un carré. Si p est impair et si (-1) et 2 ne sont pas des carrés, alors $(-1)^{(p-1)/2}=2^{(p-1)/2}=-1$ donc $(-2)^{(p-1)/2}=1$ et -2 est un carré.

b) X^5-X-1 est irréductible dans $\mathbb{F}_5[X]$. En effet il n'a pas de racine car $x^5=x$ et s'il y avait un facteur de degré 2, alors il y aurait une racine dans une extension K de degré 2 de $\mathbb{F}_5$. Comme Card $K=25$ et donc Card $K^*=24$, $x^24=1$ pour $x\neq 0$ et donc $x^25=x$. Mais si $x^5=x+1$, alors $x^{25}=(x+1)^5=1+x^5=1+2x\neq x$ car $x\neq -1$. Donc X^5-X-1 est irréductible dans $\mathbb{F}_5[X]$ et donc dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.

De même avec X^5-X^2-1. Si x est une racine dans $\mathbb{F}_5$ alors $x^5=x^2+1=x$ et on vérifie qu'il n'y a pas de tel solution. Si x est une racine dans une extension K de $\mathbb{F}_5$ de degré 2, on a $x=x^{25}=(x^2+1)^5=x^10+1=(x^2+1)^2+1=x^4+2x^2+2$. En calculant le pgcd de X^5-X^2-1 et X^4+2X^2-X+2, on tombe sur X^2+X+2.

On obtient $X^5-X^2-1=(X^3-X^2-X+2)(X^2+X+2)=\bar{P}\bar{Q}$ dans $\mathbb{F}_5[X]$ et on vérifie que les deux facteurs sont irréductibles (car ils n'ont pas de racine dans $\mathbb{F}_5$). Donc si $X^5-X^2-1=PQ$ dans $\mathbb{Z}[X]$ alors par unicité de la factorisation dans $\mathbb{F}_5[X]$, on obtient $P(0)\equiv 2 \mod 5$, or $P(0)Q(0)=-1$ est inversible dans $\mathbb{Z}$, donc $P(0)=1$ ou -1. Contradiction. X^5-X^2-1 est bien irréductible dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$.

Exercice 16. Quels sont les polynômes irréductibles de degré inférieur à 4 dans $\mathbb{F}_2[X]$.

Solution.

Exercice 17. Exemple de polynôme irréductible
$P(x)=(x-a_1)\cdots(x-a_n)-1$ est irréductible sur $\mathbb{Q}$ si les a_i sont des entiers distincts.

Solution. Il suffit de montrer qu'il est irréductible dan $\mathbb{Z}[X]$. Si $P=QR$ avec Q er R non constants, alors $Q(a_i)R(a_i)=-1$ pour tout i, donc $Q(a_i)\in\{1,-1\}$. Donc $Q+R$ s'annule en tous les a_i, or $degQ+R<n$, donc $Q=-R$. Donc $P=-Q^2$, se qui contredit la positivité du coefficient dominant.

Exercice 18. Eléments étrangers conservants le ppcm
n et m désignent deux éléments d'un anneau A factoriel.

a) Montrer qu'il existe $n'|n$ et $m'|m$, tels que $(n',m')=1$ et $\text{ppcm}(n',m')=\text{ppcm}(n,m)$.

b) si n' et m' répondent au problème et si $d=(n,m)$, alors tout p irréductible qui divise m/d divise m' et ne divise pas n'.

c) En déduire un algorithme qui calcule n' et m' en effectuant uniquement des calculs de pgcd et des divisions euclidiennes.

Solution. a) Choisissons un système de représentants d'irréductibles de A et décomposons $n=u\prod_i p_i^{n_i}$ et $m=v\prod_i p_i^{m_i}$. Si $n_i\geq m_i$ on pose $n_i'=n_i$ et $m_i'=0$ et sinon, on pose $n_i'=0$ et $m_i'=m_i$. Alors $m'=\prod_i p_i^{m_i'}$ et $n'=\prod_i p_i^{n_i'}$ conviennent.

b) Soit $a=v_p(d)$. Si p divise m/d, p^{a+1} divise m, mais ne peut pas diviser n, et donc a fortiori n', car sinon p^{a+1} diviserait $\text{pgcd}(n,m)=d$. Comme p^{a+1} divise $\text{ppcm(n, m)}=ppcmm', n'$, p^{a+1} doit diviser m' ou n'. Comme il ne peut diviser n', il divise m'. Comme n' et m' sont premiers entre eux, p ne divise pas n'.

c) On commence par calculer le pgcd d de m et n. Soit $d'=n$. On calcule ensuite le pgcd d_1 de m/d avec n, puis d_2 pgcd de $n_1=n/d_1$ avec d_1, puis le pgcd d_3 de $n_2=n_1/d_2$ avec d_2, jusqu'à ce que $d_k=1$. On pose alors $n'=n_k$ et $m'=mn/(dn')$.

Exercice 19. a) Soit R un anneau euclidien. Montrer qu'il existe $x\in R$ non inversible tel que $R^*\cup\{0\}\to R/(x)$ soit surjective.

b) Soit $A = \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. Déterminer A^* et montrer que A n'est pas euclidien.

c) Soit $x \in \mathbb{C}$. On veut montrer qu'il existe $q \in A$ tel que $|x-q| < 1$ ou $|2x-q| < 1$. On pose $x = u + iv$ avec $u, v \in \mathbb{R}$.

i) Se ramener au cas où $v \in [0, \sqrt{19}/4]$.

ii) Montrer que si $v \in [0, \sqrt{3}/2[$, il existe $q \in \mathbb{Z}$ tel que $|x-q] < 1$.

iii) Montrer que si $v \in [\sqrt{3}/2, \sqrt{19}/4]$, $\sqrt{19}/2 - 2v \in [0, \sqrt{3}/2[$ et en déduire $q \in A$ tel que $|2x-q| < 1$.

d) Soient $a, b \in A\backslash 0$. Montrer qu'il existe $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ et qui vérifient, soit $a = bq + r$, soit $2a = bq + r$.

e) Montrer que (2) est un idéal maximal de A (on pourra soit écrire la table de multiplication de $A/(2)$, soit vérifier que $X^2 + X + 5$ est un polynôme irréductible de $\mathbb{Z}/(2)[X]$).

f) Soit I un idéal de A et $b \in I - \{0\}$ minimisant $|b|$. Montrer que $2I \subset (b) \subset I$.

g) Montrer que A est principal.

Solution. a) Soit $x \in R - (R^* \cap \{0\})$ tel que $v(x)$ soit minimal. Alors si $y \in R$, il existe $q, r \in R$ tel que $y = qx + r$ (et donc $\bar{y} = \bar{r}$) et $v(r) < v(x)$, donc $r \in R^* \cap \{0\}$. Donc $\bar{y}$ est l'image de r par l'application $R^* \cup \{0\} \to R/(x)$

b) Soit $N(z) = z\bar{z} \in \mathbb{Z}$. Alors z est inversible si et seulement si $N(z) = 1$. Mais si $z = a + b\frac{1+i\sqrt{19}}{2}$, $N(z) \geq 19b^2/4 > 1$ dès que $b \neq 0$. On en déduit $R* = \{1, -1\}$.
Si x est tel que $R^* \cup \{0\} \to R/(x)$ est surjective, alors si $y \in R$, x divise y, $y+1$ ou $y-1$, et donc $N(x)$ divise $N(y)$, $N(y+1)$ ou $N(y-1)$. En prenant $y = 2$, on obtient $N(x)$ divise 1, 4 ou 9 et en prenant $y = (1 + i\sqrt{19})/2$, on obtient $N(x)$ divise 5 ou 7. Comme $1 \times 4 \times 9$ et 5×7 sont premiers entre eux, $N(x) = 1$ ce qui contredit l'hypothèse que x n'est pas inversible. Donc R n'est pas euclidien.

c) i) Soit $n \in \mathbb{Z}$ tel que $|4v/\sqrt{19} - n| \leq 1/2$. Soit $x' = x - n\frac{1+i\sqrt{19}}{2}$. Il suffit de résoudre le problème pour x'. On pose $x' = u' + iv'$. On a $v' \in [-\sqrt{19}/4, \sqrt{19}/4]$. Si $v' \geq 0$, on s'est ramené au cas voulu ; sinon, on remplace x' par $-x'$.

ii) Soit $n \in \mathbb{Z}$ tel que $|u - n| \leq 1/2$. Alors $|x-n|^2 = |u-n|^2 + |v|^2 < 1/4 + 3/4 = 1$.

iii) Comme $v \leq \sqrt{19}/4$, on a $\sqrt{19}/2 - 2v \geq 0$. Pour l'autre inégalité, il suffit de vérifier que $3\sqrt{3}/2 \geq \sqrt{19}/2$,ce qui provient du fait que $27 \geq 19$.
Du coup, $\frac{1+i\sqrt{19}}{2} - 2x$ vérifie les conditions de ii), d'où $n \in \mathbb{Z}$ tel que $|\frac{1+i\sqrt{19}}{2} - 2x - n| < 1$ et il suffit de poser $q = \frac{1+i\sqrt{19}}{2} - n$.

iv) On applique c) à $x = a/b$ et on pose $r = b(x-q) = a - bq$ ou $r = b(2x-q) = 2a - bq$ en fonction des cas.

d) Le nombre $\frac{-1+i\sqrt{19}}{2}$ est racine de $X^2 + X + 5$, d'où un morphisme surjectif $f : \mathbb{Z}[X]/(X^2+X+5) \to \mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ envoyant X sur $\frac{1+i\sqrt{19}}{2}$. Comme les deux sont des $\mathbb{Z}$-modules libres de rang 2, et que f envoie la base $(1, X)$ sur la base $(1, \frac{1+i\sqrt{19}}{2})$, c'est un isomorphisme.
Il suffit donc de montrer que $A/(2) = \mathbb{Z}[X]/(X^2+X+5, 2) = \mathbb{F}_2[X]/(X^2+X+5)$ est un corps, et donc de montrer que $P = X^2 + X + 5$ est irréductible sur $\mathbb{F}_2$. Comme le degré de P est 2 il suffit de vérifier qu'il n'y a pas de racines dans $\mathbb{F}_2$, ce qui est immédiat.

e) Remarquons que $|z|^2 \in \mathbb{N}$ donc il existe bien $b \in I - \{0\}$ minimisant $|b|^2$. Comme $b \in I$, $(b) \subset I$. Si $a \in I$. On applique c) : si $a = bq + r$, alors $r = a - bq \in I$ et par minimalité de $|b|$, $r = 0$, donc $a \in (b)$ et donc $2a \in (b)$. Si $2a = bq + r$ alors $2a \in (b)$ par le même argument.

f) On a $(2b) \subset 2I \subset (b)$, or $(b)/(2b) \simeq A/(2)$ est un A-module simple, donc $2I = (b)$ ou $(2b)$ est principal. Comme A est intègre, I est principal aussi.

2 Compléments à la feuille de TD 3

Exercice 20. Un A-module M est dit artinien si toute suite décroissante de sous-A-modules de M est stationnaire. Un anneau A est dit artinien si il est artinien en tant que A-module.

a) Montrer qu'un A-module M est artinien si et seulement si toute famille de sous-module de M admet un élément minimal.

b) Soit k-un corps. Montrer qu'une algèbre de dimension finie sur k est artinienne.

c) Soit N un sous-module de M. Montrer que M est artinien si et seulement si N et M/N sont artiniens.

d) Montrer qu'un anneau intègre est artinien si et seulement si c'est un corps.

e) Soit k un corps. Montrer qu'un k-espace vectoriel M est un k-module artinien si et seulement si il est de dimension fini.

f) On suppose dorénavant que A est un anneau artinien.

i) Montrer que tout idéal premier de A est un idéal maximal.

ii) Montrer que A n'a qu'un nombre fini d'idéaux maximaux (on pourra utiliser le lemme chinois ou un argument de comaximalité).

iii) Si $\mathfrak{m} \in \mathrm{Spec}(A)$, on note $\mathfrak{m}^\infty = \bigcap_{n\in\mathbb{N}} \mathfrak{m}^n$ et $k_\mathfrak{m} = A/\mathfrak{m}$. Munir $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ d'une structure de $k_\mathfrak{m}$-espace vectoriel et montrer qu'il est de dimension finie. En déduire que $A/\mathfrak{m}^\infty$ est un anneau noethérien.

iv) Montrer que $A \to \prod_{\mathfrak{m}\in\mathrm{Spec}(A)} A/\mathfrak{m}^\infty$ est surjective. Soit $\mathfrak{R}^\infty$ le noyau de ce morphisme. Montrer que $\mathfrak{R}^\infty \cdot \mathfrak{m} = \mathfrak{R}^\infty$ pour tout idéal maximal $\mathfrak{m}$ de A. Soit $J = \mathrm{Ann}(\mathfrak{R}^\infty) = \{x \in A, \forall y \in \mathfrak{R}^\infty, xy = 0\}$.

v) On suppose $J \neq A$. Montrer qu'il existe un idéal J' contenant J tel que J'/J soit un A-module simple et, en utilisant la question 2 de l'exercice 2, en déduire qu'il existe un idéal maximal $\mathfrak{m}$ de A tel que $J'\mathfrak{m} \subset J$. En déduire que $J' \subset \mathrm{Ann}(\mathfrak{R}^\infty)$ et obtenir une contradiction.

vi) En déduire que $A \to \prod_{\mathfrak{m}\in\mathrm{Spec}(A)} A/\mathfrak{m}^\infty$ est un isomorphisme. Montrer que A est un anneau noetherien.

g) Réciproquement soit A un anneau noethérien dont tout idéal premier est maximal.

i) Montrer qu'il existe un sous-module de A maximal M pour la propriété d'être artinien.

ii) Soit $a \in A - M$, montrer que $M + (a)$ et $M + (a)/M$ sont artiniens et en déduire une contradiction. En déduire que A est artinien.

Exercice 21. Un A-module est dit simple si il a exactement deux sous-modules (0 et lui-même). Un A-module M est dit de longueur finie si il existe une suite de sous-modules

$$0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_m = M$$

telle que, pour tout $1 \leq i \leq n$, M_i/M_{i-1} soit simple (une tel suite est appelé suite de décomposition de M et les M_i/M_{i-1} sont).

a) Soit I un idéal de A. Montrer que A/I est un A-module simple si et seulement si I est un idéal maximal.

b) Soit M un module simple. Montrer qu'il existe un idéal maximal $\mathfrak{m}$ tel que M soit isomorphe à $A/\mathfrak{m}$.

c) Montrer que si M est un module de type fini non nul, alors M a un sous-module N tel que M/N soit simple.

d) Montrer qu'un A-module est de longueur fini si et seulement si il est noethérien et artinien.

e) Montrer que si M est de longueur fini, la longueur m de la suite de décomposition ne dépend pas du choix de la suite de décomposition et que les facteurs non plus à permutation près. Plus précisément, si

$$0 = N_0 \subset N_1 \subset N_2 \subset \cdots \subset N_n = M$$

est une autre suite de décomposition, montrer que $m = n$ et qu'il existe $\sigma \in \mathfrak{S}_n$ tel que M_i/M_{i-1} soit isomorphe à $N_{\sigma(i)}/N_{\sigma(i)-1}$.

Exercice 22. Soit A un anneau local, d'anneau local, d'idéal maximal $\mathfrak{m}$. Soit $k = A/\mathfrak{m}$

a) Soit P un A-module projectif (cf. TD 3 exo 9) de type fini.

b) Montrer qu'il existe $n \in \mathbb{N}$ et un A-module de type fini P' tel que $P \oplus P' \simeq A^n$. On identifie dorénavant $P \oplus P'$ et A^n.

c) Munir $P/\mathfrak{m}P$ et $P'/\mathfrak{m}P'$ d'une structure de k-espace vectoriel. Soit $(\bar{e}_i)_{i\in I}$ et $(\bar{e}'_j)_{j\in J}$ une base de $P/\mathfrak{m}P$ et $P'/\mathfrak{m}P'$ respectivement. Montrer que $\mathrm{Card}(I) + \mathrm{Card}(J) = n$

d) Soit e_i un antécédent de $\bar{e}_i$ par le morphisme $P \to P/\mathfrak{m}P$ et e'_j un antécédent de $\bar{e}'_j$ par le morphisme $P' \to P'/\mathfrak{m}P'$. Montrer que $(e_i)_{i\in I}$ et $(e'_j)_{j\in J}$ sont des familles génératrices de P et P' (on pourra appliquer le lemme de Nakayama (TD 2 exo 13) à $P/\langle e_i\rangle_{i\in I}$).

e) En déduire deux applications surjectives $A^{\mathrm{Card}(I)} \to P$ et $A^{\mathrm{Card}(J)} \to P'$. En déduire une application surjective $f : A^n \to A^n$.

f) Montrer que $\det f$ est inversible (on pourra réduire modulo $\mathfrak{m}$). Montrer que f est un isomorphisme.

g) En déduire que P est un module libre.

Exercice 23. Soit A l'anneau des fonctions continues de $\mathbb{R}$ vers $\mathbb{R}$ qui sont π-périodiques. Soit $P = \{g \in \mathcal{C}^0(\mathbb{R}, \mathbb{R}), g(x+\pi) = -g(x)\}$.

a) Munir P d'une structure de A-module via $(f.g)(x) = f(x)g(x)$.

b) Montrer que $\Big((\cos, \sin), (\sin, -\cos)\Big)$ forme une base du A-module $P \oplus P$.

c) Montrer que P n'est pas un A-module libre (on pourra commencer par montrer que toute famille d'au moins deux éléments de P est liée).