Anneaux commutatifs

Déf. 1. (Anneau).

Un anneau A est un ensemble non vide A muni de 2 opérations internes $+$ et $\cdot$ tels que :

1) Pour "$+$", A est un groupe abélien
2) "$\cdot$" est associative.
3) "$\cdot$" est distributive par rapport à "$+$" (à droite et à gauche).

0 = zéro de A = l'élément neutre de $+$

$-x$ = le symetrie de x pour $+$, $x \in A$.

Déf. 2. Soit $(A, +, \cdot)$ un anneau.

- A est unitaire si il possède un élément neutre pour "$\cdot$" "on le note souvent 1"
- A est commutatif si la loi "$\cdot$" est commutative.

Exemples :

1) $(\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire
2) $(2\mathbb{Z}, +, \times)$ " " " " non unitaire commutatif
3) Pour $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau unitaire commutatif et fini. $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$.

exemple : $n = 6$, calculer $\bar{4} + \bar{3}$, $\bar{2} \times \bar{3}$.

4) Pour $n \in \mathbb{N}^*$, $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ est un anneau unitaire non commutatif - avec

$0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ et $1 = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} = I_n$

Remarquer que si on prend, par exemple, $n = 2$, on a

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(le produit de 2 matrices non nulles est une matrice nulle)

5) Soit $d \in \mathbb{Z}^*$, $d \neq 1$. $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \;/\; a, b \in \mathbb{Z}\}$ et $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$, pour $+$ et $\times$, sont des anneaux commutatifs unitaires.

Déf 3.

- Un élément $a \neq 0$, d'un anneau commutatif A est un diviseur de zéro, s'il existe $y \neq 0$ dans A tel que $xy = 0$.
- Un anneau commutatif est intègre si il ne possède pas de diviseur de zéro. (c.à.d. si $a \neq 0$ et $b \neq 0$, alors $ab \neq 0$, pour $a, b \in A$).

Exemples.

1) $\mathbb{Z}$ est un anneau intègre
2) Dans $\mathbb{Z}/6\mathbb{Z}$, $\bar{2}$ est un diviseur de zéro, donc $\mathbb{Z}/6\mathbb{Z}$ est non intègre.
3) L'exemple 4 précédent, $M_2(\mathbb{R})$ est non intègre car $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ est un diviseur de zéro.

à retenir (exercice)

$\mathbb{Z}/n\mathbb{Z}$ est intègre $\Leftrightarrow$ n est premier.

Déf 4. Soit A un anneau unitaire, un élement $a \in A$ est appelé unité s'il admet un inverse $\bar{a}^1 \in A$ pour la multiplication.

Exemples:

- Les seuls unités de $\mathbb{Z}$ sont $1, (-1)$.
- Tout élément non nul de $\mathbb{Q}$ est un(e) unité
- Si $A = \{0\}$, 0 est un(e) unité. (si $A \neq \{0\}$, 0 est non unité).
- exercice: Soit $\mathbb{Z}[\sqrt{2}]$. montrer que $3 + 2\sqrt{2}$, $-3 - 2\sqrt{2}$ sont des éléments unités.

Pour un anneau unitaire A, notons par U l'ensemble des unités de A.

Proposition $(U, \cdot)$ est un groupe (pour la multiplication de A)

Dém. évidente.

Déf 5. Le groupe $(U, \cdot)$ est appelé le groupe des unités de A.

Exemples
- $U(\mathbb{Z}) = \{1, -1\}$
- $U(\mathbb{Q}) = \mathbb{Q}^\times = \mathbb{Q} - \{0\}$
- $U(\mathbb{Z}/5\mathbb{Z}) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$
- $U(\mathbb{Z}/4\mathbb{Z}) = \{\bar{1}, \bar{3}\}$.

à retenir (exercice)

$\bar{x}$ est unité dans $\mathbb{Z}/n\mathbb{Z} \iff (x, n) = 1$

Déf. 6. Un corps est un anneau commutatif unitaire (non trivial) dont tout élément non nul est un élément unité.

Remarque
- Si K est un corps, alors $U(K) = K^\times = K - \{0\}$.
- tout corps est un anneau (~~commutatif~~) intègre.

Exemple important

Soient $(A, +, \cdot)$ un anneau et X une indéterminée (X est un symbole)

Un polynôme en X (d'indéterminée X) à coefficients dans A est une somme formelle

$$a_0 + a_1 X + a_2 X^2 + \cdots$$

avec $a_i \in A$ pour tout i et $a_i = 0$ pour i suffisamment grand.

$A[X]$ = l'ensemble des polynômes en X à coefficients dans A.

Addition et multiplication des polynômes

$$f = a_0 + a_1 X + a_2 X^2 + \cdots \in A[X]$$
$$g = b_0 + b_1 X + b_2 X^2 + \cdots$$

$f + g \in A[X]$ est défini par

$$f + g = (a_0 + b_0) + (a_1 + b_1) X + \cdots$$

$f, g \in A[X]$ est défini par :

$$f \cdot g = c_0 + c_1 X + c_2 X^2 + \cdots$$

avec :
$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0$$
$$\vdots$$
$$c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_{n-1} b_1 + a_n b_0 = \sum_{k=0}^{n} a_k b_{n-k}$$

on a les résultats suivants (exercice)

- $(A[X], +, \cdot)$ est un anneau.
- Si A est unitaire d'unité 1, alors $A[X]$ est unitaire d'élément unité $1 = 1 + 0X + 0X^2 + \cdots$
- Si A est intègre, alors $A[X]$ est intègre.
- Si K est un corps, alors $K[X]$ est un anneau commutatif unitaire intègre. ($K[X]$ n'est pas un corps. car X n'admet pas un inverse).

Déf. 7. (degrés d'un polynôme)

$f \in A[X]$. Si $f \neq 0$, $f = a_0 + a_1 X + \cdots + a_n X^n$, $a_n \neq 0$

n est le degrés de f et on écrit $\deg(f) = n$.

Convention : $\deg(0) = -\infty$

Proposition

Soient A un anneau, X indéterminé sur A et $f, g \in A[X]$

1) $\deg(f+g) \leq \max(\deg(f), \deg(g))$ avec égalité si $\deg(f) \neq \deg(g)$.

2) Si A est intègre, alors on a $\deg(fg) = \deg(f) + \deg(g)$

Dém. exercice.

Thm (Division euclidienne)

Soient K un corps, X indéterminé sur K et $f, g \in K[X]$ tels que $g \neq 0$. Alors il existe $(q, r) \in (A[X])^2$ unique t.q.

- $f = qg + r$ et
- $\deg(r) < \deg(g)$

Polynôme à plusieurs indéterminés (variables)

A anneau, X indéterminée sur $A \longrightarrow A[X]$

$$f \in A[X] \iff f = c_0 + c_1 X + \cdots + c_n X^n \; ; \quad c_i \in A$$

$A[X]$ anneau, Y indéterminé sur $A[X] \longrightarrow A[X][Y]$

$$f \in A[X][Y] \iff f = a_0(X) + a_1(X)Y + a_2(X)Y^2 + \cdots + a_n(X)Y^n$$

$$a_i(X) \in A[X].$$

$$\iff f = b_{00} + b_{01}X + b_{10}Y + b_{20}X^2 + b_{11}XY + b_{02}Y^2 + \cdots$$

$XY = YX \Rightarrow A[X][Y] = A[Y][X] = A[X,Y]$

$\cdots\cdots$ $A[X_1, \ldots, X_n]$

Exercice (K commutatif)

I) Soit K un corps, $f \in K[X]$ non constant, $a \in K$

1) Montrer que a est une racine de f dans K ($f(a)=0$) ssi $f = (X-a)\,g(X)$ pour $g \in K[X]$.

2) Montrer que si $\deg(f) = n \geq 1$ alors f possède au plus n racines dans K.

II) Soit A un anneau commutatif, $n \in \mathbb{N}^*$

- Montrer que pour $a, b \in A$, on a :

$$(a+b)^n = \sum_{k=0}^{n} C_n^k\, a^{n-k} b^k, \text{ où } C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

- Supposons que $A = \mathbb{Z}/p\mathbb{Z}$, p premier

Montrer que pour $a, b \in \mathbb{Z}$, on a,

$$(a+b)^p \equiv a^p + b^p \; [p].$$

III) 1- Montrer que $\mathbb{Z}[i] = \{ a+bi \,/\, a, b \in \mathbb{Z} \} \subset \mathbb{C}$ muni de l'addition et la multiplication dans $\mathbb{C}$ est un anneau commutatif unitaire intègre

2)- Pour $\alpha = a+bi \in \mathbb{Z}[i]$, on pose $\phi(\alpha) = a^2 + b^2$

- Montrer que $\phi(\alpha\beta) = \phi(\alpha).\phi(\beta)$, pour tout $\alpha, \beta \in \mathbb{Z}[i]$

$\phi(\alpha) = 0 \Leftrightarrow \alpha = 0$.

- Montrer que α est un élément unité de $\mathbb{Z}[i]$ ssi $\phi(\alpha) = 1$
- Montrer que $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

Sous-anneau & Idéaux et anneau quotient

Déf. 1. (sous-anneau).
Soit A un anneau. Une partie S de A est un sous-anneau de A si S est un anneau pour les lois internes de A.

Exemples
- $\mathbb{Z} \leq \mathbb{Q}$, $\mathbb{Q} \leq \mathbb{R}$, $2\mathbb{Z} \leq \mathbb{Z}$, $\mathbb{Z}[\sqrt{d}] \leq \mathbb{Q}[\sqrt{d}]$.
- Si A est un anneau, $\{0\}$ et A sont des sous-anneaux de A. (s.a. triviaux).
- $\langle x^2+1 \rangle = \{(x^2+1) f(x) \mid f \in K[x]\}$ est un s.a. de $K[x]$, avec K corps commutatif.

Théorème. Soit $\emptyset \neq S \subset A$ anneau. Alors S est un s.a. de A ssi $\forall a, b \in S$, on a $a-b \in S$, $a.b \in S$.

Preuve.
($\Rightarrow$) evidente.
($\Leftarrow$) $a-b \in S \Rightarrow S \leq_g (A,+)$.
$a.b \in S \Rightarrow$ S est stable par "$.$".

Déf. 2. (Idéal). Soit A un anneau, un idéal (bilatère) de A est un sous-anneau I de A tel que si $a \in A$, $i \in I$, alors $ia \in I$ et $ai \in I$.

Rq. I idéal de $A \Leftrightarrow \begin{cases} \forall i, j \in I, (i-j) \in I \\ \forall i \in I, \forall a \in A, ia \in I \text{ et } ai \in I. \end{cases}$

Exemples.
- Si A est un anneau, $\{0\}$, A sont des idéaux (triviaux)
- $A = \mathbb{Z}$, $I = n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$, $n \geq 0$
- K corps commutatif, X indéterminée sur K, $f \in K[X]$
$\langle f(x) \rangle = fK[x] = \{f \cdot g \mid g \in K[x]$ est un idéal de $K[x]\}$
- K corps commutatif, $K[X,Y]$
$(X,Y) = \{X \cdot f + Y \cdot g \mid f, g \in K[X,Y]\}$ est un idéal de $K[X,Y]$.
- important Si $a \in A$ anneau commutatif
$\langle a \rangle = \{ax \mid x \in A\} = aA$ idéal de A.

Rq. Tout idéal est un sous-anneau mais la réciproque est fausse.

$\mathbb{Z}$ s. anneau de $\mathbb{Q}$, mais il n'est pas idéal de $\mathbb{Q}$.

$1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$.

Anneau quotient

Soit A un anneau, I idéal de A.

Pour $a \in A$, $a + I = \{ a + i \mid i \in I \}$.

$(a + I) = (b + I)$ ssi $(a - b) \in I$.

$0 + I = I$.

$a \sim b \Leftrightarrow a + I = b + I \Leftrightarrow (a - b) \in I$

$\sim$ est une relation d'equivalence sur A, de plus on a

$\bar{a} = [a] = a + I$.

$A/_\sim = A/_I = \{ a + I \mid a \in A \}$.

Sur $A/_I$ on définit deux lois "internes":

l'addition: $(a+I) + (b+I) = (a+b) + I$.

la multiplication: $(a+I) \cdot (b+I) = (a \cdot b) + I$

Proposition Soit A un anneau, et soit I un idéal de A

L'ensemble A/I muni des lois précédentes est un anneau (appelé anneau quotient de A par I).

Preuve : exercice.

$\bar{0} = 0 + I = I$, $-(a+I) = (-a) + I$.

Rq. Si A est commutatif, alors A/I est commutatif

Si A est unitaire d'unité 1, alors A/I est unitaire d'unité $1 + I$.

Exemples: • $A = \mathbb{Z}$, $I = n\mathbb{Z}$, $A/I = \mathbb{Z}/n\mathbb{Z}$.

• A anneau,

$I = \{0\} \rightarrow a + \{0\} \rightarrow a$, $A \equiv A/I$.

$I = A \rightarrow A/I \equiv \{0\}$
$= \{A\}$

$a + I = I \Leftrightarrow a \in I$

$1 \in I \Leftrightarrow I = A$.

$x \in U(A)$: $x \in I \Leftrightarrow I = A$

(~ 2)

Exemple très important

Soient K un corps commutatif, $A = K[X]$, $f \in A[X]$ de degrés $n \geq 1$.

$I = (f) = fK[X]$.

$$A/I = K[X]/(f) = \{ g + I \mid g \in K[X] \}.$$

Rappelons que $g + I = h + I \Leftrightarrow (g - h) \in I$.

Par la division euclidienne de $g \in K[X]$ par $f(X) \in K[X]$,

$\exists !\ q(X), r(X) \in K[X]$ t.q. $g = f \cdot q + r$ avec

$$r = 0 \quad \text{ou} \quad 0 \leq \deg(r) < \deg(f).$$

Comme $f \cdot q \in I$, on a $f \cdot q + I = 0 + I = I$.

Donc : $g + I = f \cdot q + r + I = r + I$.

chaque classe $g + I$ peut être écrite de la forme $r + I$, où

$r(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$, $a_i \in K$.

De plus si $r + I = r' + I \Rightarrow r - r'$ est multiple de f

mais comme $\deg(r), \deg(r') < \deg(f)$, on a $r = r'$

c'est à dire l'écriture $r + I$ de $g + I$ est unique.

$$\therefore \quad \boxed{\frac{K(X)}{(f)} = \{ a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + I \mid a_i \in K \},\ n = \deg(f).}$$

cas particulier $A = \mathbb{Q}[X]$, $f(X) = X^2 - 2$

$$\frac{\mathbb{Q}[X]}{(X^2 - 2)} = \{ a_0 + a_1 X + I,\ a_0, a_1 \in \mathbb{Q} \}.$$

On a :

$$(a_0 + a_1 X + I) + (b_0 + b_1 X + I) = (a_0 + b_0) + (a_1 + b_1) X + I.$$

$$(a_0 + a_1 X + I) \cdot (b_0 + b_1 X + I) = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + a_1 b_1 X^2 + I$$

$$= a_0 b_0 + (a_0 b_1 + a_1 b_0) X + a_1 b_1 X^2 - 2 a_1 b_1 + 2 a_1 b_1 + I$$

$$= (a_0 b_0 + 2 a_1 b_1) + (a_0 b_1 + a_1 b_0) X + a_1 b_1 (X^2 - 2) + I$$

$$= (a_0 b_0 + 2 a_1 b_1) + (a_0 b_1 + a_1 b_0) X + I.$$

Proposition Soient A un anneau, I un idéal de A.

- Si S est un s/anneau de A contenant I, alors S/I est un sous-anneau de A/I,
- Reciproquement, Tout s/anneau de A/I est de la forme S/I où S est un s/anneau de A contenant I.

Dém.

- $S/I = \{s+I : s \in S\} \subseteq A/I$. Pour $s+I,\ t+I \in S/I$, on a
  $(s+I)-(t+I) = (s-t)+I \in S/I$ car $(s-t) \in S$
  $(s+I).(t+I) = st+I \in S/I$ car $s.t \in S$
  $\Rightarrow$ S/I est un s/anneau de A/I.
- Réciproquement, soit $U \subseteq A/I$ un s/anneau. Soit $S = \{s \in A / s+I \in U\}$.
  Alors S est un s/anneau de A qui contient I et $U = S/I$.

Idéal premier et idéal maximal.

Soit A un anneau commutatif unitaire

Déf. (idéal premier). Soit I un idéal de A, $I \neq A$.
On dit que l'idéal I est premier si pour tout $a, b \in A$
$ab \in I$, alors on a $a \in I$ ou $b \in I$.

Exemples: $A = \mathbb{Z}$.

1) Soit p premier, alors $(p) = p\mathbb{Z}$ est un idéal premier.
Si $(ab) \in (p) \Leftrightarrow p/ab \overset{\text{Euclid}}{\Rightarrow} p/a$ ou p/b i.à.d. $a \in (p)$ ou $b \in (p)$.

2) $(4) = 4\mathbb{Z}$ n'est pas premier car $2 \notin (4)$ mais $2.2 \in (4)$.

3) (X) est 1ère car si $fg \in (X) \Rightarrow f(0)g(0) = 0 \Rightarrow f(0) = 0$ ou $g(0) = 0$
$\Rightarrow X/f$ ou X/g.

Théorème.
Soit I un idéal d'un anneau commutatif unitaire A
$I \neq A$. Alors I est premier $\Leftrightarrow$ A/I est un anneau intègre

Dém. $(\Rightarrow)$ $(a+I).(b+I) = 0+I \Leftrightarrow ab+I = 0+I \Leftrightarrow ab \in I \Leftrightarrow$
$a \in I$ ou $b \in I \Leftrightarrow a+I = I$ ou $b+I = I$
c.à.d. A/I est intègre.

$(\Leftarrow)$ $ab \in I \Rightarrow ab+I = I = 0+I = (a+I).(b+I)$
$\Rightarrow a+I = I$ ou $b+I = I \Rightarrow a \in I$ ou $b \in I$
$\Rightarrow I$ premier.

Déf (idéal maximal). un idéal I de A est dit maximal
si : $I \neq A$ et si $I \subset J \Rightarrow J = I$ ou $J = A$.

Exemple: p premier, $(p) = p\mathbb{Z}$ est maximal de $\mathbb{Z}$.
$p\mathbb{Z} \subset a\mathbb{Z} \Rightarrow p \in a\mathbb{Z}$ $a/p \Rightarrow a = 1$ (donc $a\mathbb{Z} = \mathbb{Z}$)
ou $a = p$ ($a\mathbb{Z} = p\mathbb{Z}$).

Théorème.
I est un idéal maximal de A ssi A/I est un Corps

Dém. exercice.

Exemples :

$I = n\mathbb{Z}$ est maximal dans $\mathbb{Z} \Leftrightarrow \frac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps $\Leftrightarrow n$ est premier.

Théorème

si I est maximal, alors I est premier

Déf. I maximal $\Rightarrow A/I$ corps $\Rightarrow A/I$ intègre $\Rightarrow I$ premier.

Exercice.

Soit $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$.

- Décrire les éléments de $\mathbb{Z}_2[x]/(f)$. Dresser les tables d'addition et de multiplication dans $\mathbb{Z}_2[x]/(f)$.
- Montrer que $\mathbb{Z}_2[x]/(f)$ est un corps à 4 éléments.

Opérations sur les idéaux : A unitaire commutatif

1) L'Idéal engendré par une partie $S \subset A$ est l'intersection de tous les idéaux de A contenant S. On vérifie aisément que :

$$(S) = \left\{ \sum_{i \in I} a_i r_i \ , \ I \text{ fini}, \ s_i \in S, \ r_i \in A \right\}$$

- Si $S = \{a_1, a_2, \dots\}$, $(S) = (a_1, a_2, \dots)$
- Si $S = \{a\}$, $(a) = aA$: idéal principal

2) La somme de deux idéaux I et J est l'idéal

$$I + J = \{ i + j \ / \ i \in I \text{ et } j \in J \}$$

3) Le produit de deux idéaux I et J est l'idéal engendré par $\{ab / a \in I \text{ et } b \in J\}$

$$I.J = \left\{ \sum_{i \in I} a_i b_i \ , \ I \text{ fini}, \ a_i \in I, \ b_i \in J \right\}$$

Remarquer que $IJ \subset I \cap J$.

(1 ∈ I + J)

- Deux idéaux I et J sont étrangers (ou copremiers) si $I + J = A$
- De même $I_1, I_2, \dots, I_n$ sont 2 à 2 étrangers si $I_i + I_j = A$, pour tous $i \neq j$.
- Si $I + J = A$ alors $IJ = I \cap J$.

($I_1, \dots, I_n$ sont 2 à 2 étrangers, alors $\prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$)

Dém 1) $IJ \subset I \cap J$ évident

Soit $x \in I \cap J$, $I + J = A$.

Donc $\exists \ i, j \in I, J$ t.q. $1 = i + j$

$\Rightarrow x = xi + xj \in I.J$

2) Si $I_1, \dots, I_n$ sont 2 à 2 étrangers, alors I_i et $\prod_{\substack{j=1 \\ j \neq i}}^{n} I_j$ sont étrangers.

Pour tout $j \neq i$, $I_i + I_j = A$

$\Rightarrow \exists \ a_i^j \in I_i, \ a_j \in I_j \ : \ a_i^j + a_j = 1$

$\Rightarrow \prod_{j \neq i} (a_i^j + a_j) = 1$

Or a $1 \in I_i + \prod_{j \neq i} I_j \Rightarrow I_i + \prod_{j \neq i} I_j = A$.

(car $I = A \Leftrightarrow 1 \in I$)

Théorème des restes chinois. Soit A un anneau unitaire commutatif. Soient $x_1, x_2, \dots, x_n$ des éléments de A et $I_1, I_2, \dots, I_n$ des idéaux de A 2 à 2 étrangers, alors il existe $x \in A$ tel que $x - x_i \in I_i$, $\forall i = \overline{1,n}$

Rq. Cela veut dire que l'application

$$\varphi : A \longrightarrow A/I_1 \times A/I_2 \times \dots \times A/I_n \text{ est surjective}$$

$$\left(\ker \varphi = \bigcap_{i=1}^{n} I_i = \prod_{i=1}^{n} I_i\right)$$

Dém. $n = 2$, $\exists\, a_1 \in I_1$, $a_2 \in I_2$ t.q. $a_1 + a_2 = 1$

On prend $x = a_1 x_2 + a_2 x_1$

. Pour $n > 2$. $I_1 + \left(\prod_{i \neq 1} I_i\right) = A$ (d'après ce qui précède).

$$\Rightarrow \exists\, y_1 \in A \text{ t.q. } \begin{cases} y_1 - 1 \in I_1 \\ y_1 \in \prod_{i \neq 1} I_i \end{cases}$$

$$\left(\Rightarrow y_1 - 1 \in I_1 \text{ et } y_1 \in I_i,\ i \neq 1\right)$$

De même $\exists\, y_2, \dots, y_n$ t.q.

$$y_i - 1 \in I_i \text{ et } y_i \in \prod_{j \neq i} I_j, \text{ pour } i \geq 2$$

L'élément $x = x_1 y_1 + x_2 y_2 + \dots + x_n y_n$ répond à notre question.

Exemple résoudre le système (dans $\mathbb{Z}$).

$$\begin{cases} x \equiv 1\ [3] \\ x \equiv 2\ [5] \\ x \equiv 4\ [7] \end{cases}$$

$$\begin{cases} y_1 \equiv 1\ [3] \\ y_1 \equiv 0\ [35] \end{cases}$$

$y_1 = 35k = 3s + 1$

Calcul de k (ou s)

$35k = 3s + 1$

$\overline{35} \cdot \overline{k} = \overline{1}$ dans $\mathbb{Z}_3$

$\left(\overline{k} = \left(\overline{35}\right)^{-1}[3]\right)$

Bézout

$35(-1) + 3(12) = 1$

dans $\mathbb{Z}_3$: $\overline{35} \cdot \overline{(-1)} = \overline{1}$

$\overline{35} \cdot \overline{2} = \overline{1}$

$\overline{k} = \overline{2}$, $k = 3t + 2$.

$$y_1 = 35(3t + 2), \quad t \in \mathbb{Z}$$

(**)

Homomorphisme d'anneaux

Déf. 1. Soient A et B deux anneaux, $f: A \to B$ une application. f est un homomorphisme d'anneaux si : Pour tout $(a,b) \in A^2$:

$$f(a+b) = f(a) + f(b) \quad \text{et} \quad f(ab) = f(a) \cdot f(b)$$

Déf. 2. Un homomorphisme bijectif $f: A \to B$ est appelé isomorphisme. On dit que A et B sont isomorphes et on écrit $A \approx B$ ou $A \simeq B$.

Exemples :

1) $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \overline{x}$ est un homo. surjectif.

2) $\mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$, $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ est un isomorphisme

3) $\mathbb{Q}[X]/(X^2-2) \longrightarrow \mathbb{Q}(\sqrt{2})$ est un isomorphisme

$$a_0 + b_0 X + (X^2-2) \longmapsto a+b\sqrt{2}$$
$$\overline{X} \longmapsto \sqrt{2}$$

$$\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[X]/(X^2-2).$$

4) I idéal de A, $\pi: A \to A/I$, $x \mapsto x+I$ est l'homomorphisme canonique de A sur A/I (surjectif)

5) $S \leq_{ann} A$, $i: S \to A$ homomorphisme (mono. canon.)

Théorème. Soit $f: A \to B$ un homomorphisme d'anneaux.

1. Si S est un s/anneau de A, alors $f(S) \leq_{ann} B$.
2. $\ker f = \{x \in A / f(x) = 0\}$ est un idéal de A.

Preuve 1. $x = f(a)$, $y = f(b) \in f(S)$, $a, b \in S$

$$x - y = f(a) - f(b) = f(a-b) \in f(S)$$
$$xy = f(a) \cdot f(b) = f(ab) \in f(S).$$

2. $x, y \in \ker f$, $a \in A$.

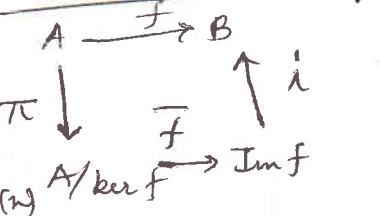
$$f(x-y) = f(x) - f(y) = 0 \Rightarrow x - y \in \ker f$$

$$\begin{cases} f(ax) = f(a) \cdot f(x) = f(a) \cdot 0 = 0 \\ f(xa) = 0 \end{cases} \Rightarrow ax \in \ker f.$$

Théorème (1er théorème d'isomorphisme d'anneaux).

Soit $f: A \to B$ un homomorphisme. $\pi: A \to A/\ker f$ et $i: \mathrm{Im} f \to B$ sont resp. l'épi. et le mono. canoniques.

Alors il existe un unique isomorphisme $\overline{f}: A/\ker f \to \mathrm{Im} f$ t.q. $i \circ \overline{f} \circ \pi = f$.



À retenir : $A/\ker f \simeq \mathrm{Im} f$.

i : injection canonique (monomorphisme)

Preuve : il suffit de prendre $\overline{f}(\overline{x}) = f(x)$

Ex. Sachant que le 1er Janvier 1994 est un samedi, quel jour de la semaine tombe le 144ème Jour de l'année ?

Solution: chaque jour de la semaine revient tous les 7 jours. Par conséquent si on numérote les jours de 1 à 365, deux jours occupent la même position dans la semaine ssi leurs numéros sont congrus modulo 7. Comme $144 \equiv 4 [7]$, le 144ème jour de l'année occupe la même position que le 4ème, qui est un mardi

$\overline{1}$ = samedi = $\{1, 8, 15, \dots\}$
$\overline{2}$ = dimanche = $\{2, 9, 16, \dots\}$
$\overline{3}$ = lundi = $\{3, 10, 17, \dots\}$
$\overline{4}$ = mardi = $\{4, 11, 18, \dots, 144, \dots\}$ - - -

Fonction Indicatrice d'Euler:

$n > 1$. $\varphi(n) = |\{m \in \mathbb{N} : 1 \le m \le n, (m, n) = 1\}|$

. si p est premier $\varphi(p) = p - 1$.

. ~~si p est premier~~ φ ~~de exemple~~ si $(a, b) = 1$,

$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$

. si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $\varphi(n) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_k^{\alpha_k})$

$$= p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1) = n \prod_{\substack{p_k \text{ premier} \\ p/n}} \left(1 - \frac{1}{p_k}\right)$$

. Remarque: $\varphi(n) = \left| \cup\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) \right| = \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$.

Si $(a, n) = 1$, alors $a^{\varphi(n)} \equiv 1 [n]$ Théorème d'Euler.

? $14641 = 11^4 = 11^{\varphi(12)} \equiv 1 [12]$

Cas particulier si p est premier et $p \nmid a$, alors $a^{p-1} \equiv 1 [p]$.

1er Janvier : 2015 → Jeudi

144ème

Homework N° 1.

ALGEBRA.

$e^{i\frac{2\pi}{3}}$.

Let $\xi = (-1+\sqrt{3}\,i)/2$ be a primitive - cube root of 1, and let $\mathbb{Z}[\xi] = \{a_0 + a_1\xi + \dots + a_r\xi^r \mid a_i \in \mathbb{Z},\ r \geq 0\}$

- Show that $\mathbb{Z}[\xi]$ is an integral domain with respect to addition and multiplication in $\mathbb{C}$.
- Show that $\mathbb{Z}[\xi] = \{a + b\xi \mid a, b \in \mathbb{Z}\}$ (prove by induction that $\xi^n \in \{a+b\xi \mid a, b \in \mathbb{Z}\}$, for all $n \in \mathbb{N}$)
- Define, for $\alpha = a + b\xi \in \mathbb{Z}[\xi]$, the norm of α, denoted $N(\alpha)$, by

$$N(\alpha) = a^2 - ab + b^2$$

Show that $\forall\, \alpha, \beta \in \mathbb{Z}[\xi]$, we have

$$N(\alpha\beta) = N(\alpha) \cdot N(\beta)$$

$N(\alpha) = 0$ if - and only if $\alpha = 0$

- Show that $N(\alpha) = 1$ if - and only if α is - a unit of $\mathbb{Z}[\xi]$.

- Deduce that the units of $\mathbb{Z}[\xi]$ are $\pm 1, \pm\xi, \pm\xi^2$.

Anneaux Principaux

1. Divisibilé dans 1 ann. intègre.

A 1 ann. comm. unit. intègre.

Def 1. $a, b \in A$, (a divise b) ou (b mult. de a)
$a|b \iff \exists q \in A : b = qa$

Rq : 1) La relation $(..|..)$ est 1 relation de préordre (reflex + transit) mais non antisy.

2) $a|b$ et $b|a \iff \exists u \in A^* = U(A)$ $b = au$.

3) **Rappel :** $(a) = aA = \{ax \mid x \in A\}$ idéal engendré par $a \in A$.

- $(a) \subset (b) \iff b|a$
- $(a) = (b) \iff a|b$ et $b|a \iff \exists u \in A^* : b = au$.

Def 2 : $(a, b) \in A^2$ sont associés ssi $(a) = (b)$ ($\iff a|b$ et $b|a \iff b = au, u \in A^*$)

Exemples : 1) $A = \mathbb{Z}$, $(-2)|4$ et $(-2), +2)$ associés

2) . $A = K[x]$, $a \in K$, $(X - a)$ et $c(X-a)$ $c \in K^*$ associés

. $A = \mathbb{Z}[x]$, $x+1 / x^2+1$.

Rq : (... est associé a ..) est 1 r. d'équivalence.

2. Anneaux principaux : A ann. unit. com. intègre

Def 1. L'idéal I est principal si $I = (a)$, $a \in A$

Exple :
- tout idéal de $\mathbb{Z}$ est principal
- $(4, 6) = 4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z} = (2)$
- $(a_1, \dots, a_n) = \sum_{i=1}^{n} a_i \mathbb{Z} = (a_1 \wedge \dots \wedge a_n)\mathbb{Z}$.

Def 2. Un ann. est principal s'il est intègre et tous ses idéaux sont principaux

Exples :
* $A = \mathbb{Z}$ est 1 ann. principal $\forall I = (n)$
* K corps $\iff K[x]$ est principal (preuve voir T.D)

3. PGCD dans un ann. principal :

A principal, $(a) + (b)$ est principal $= (\delta)$

δ n'est pas unique car $(\delta) = (\delta') \iff \exists u \in U(A) : \delta' = \delta u$

si $\delta' = \delta u$ alors $(a) + (b) = (\delta) = (\delta') = (\delta u)$, $u \in U(A) = A^*$

Def : Un élt δ vérifiant $(a)+(b)=(\delta)$ est parfaitement déterminé à 1 coeff. multiplicatif inversible près. on l'appelle "le" pgcd $(a,b) = a\wedge b = \delta$.

Ex :
* $A=\mathbb{Z}$, $(4)+(6)=(2)=(-2)$, $\delta=2$ ou $\delta=-2$
* $A=\mathbb{Q}[X]$, $(X^2-1)+(X^2-2X+1)=(X-1)$.

Thm :

$$\left[\delta = pgcd(a,b)\right] \overset{1}{\Longleftrightarrow} \left[d/\delta \Leftrightarrow d/a \text{ et } d/b\right] \overset{2}{\Longleftrightarrow} \left\{\begin{array}{l} \cdot\ \delta \text{ divise } a \text{ et } b \\ \cdot\ d/a \text{ et } d/b \Rightarrow d/\delta. \end{array}\right.$$

② voir TD.

① ($\Rightarrow$) $d/\delta \Leftrightarrow (\delta)\subset(d) \Leftrightarrow (a)+(b)\subset(d) \Leftrightarrow (a)\subset(d)$ et $(b)\subset(d) \Leftrightarrow d/a$ et d/b

($\Leftarrow$) si $[d/\delta \Leftrightarrow d/a \text{ et } d/b]$, $\delta_0 = pgcd(a,b)$

Le sens direct ($①\Rightarrow$) $d/\delta_0 \Leftrightarrow d/a$ et d/b de sorte que $(d/\delta \Leftrightarrow d/\delta_0)$

ou encore δ_0/δ et δ/δ_0 , $\Rightarrow$ δ, δ_0 sont associés.

Thm. *A multiplication près par 1 élt inv.*

1) $a\wedge b = b\wedge a$, $\forall a,b\in A$.
2) $(a\wedge b)\wedge c = a\wedge(b\wedge c)$ " "
3) $xa\wedge xb = x(a\wedge b)$, $a,b,x\in A$

. 1, 2) utiliser la def. $(a)+(b)=(a\wedge b)$

. $(xa\wedge xb) = (xa)+(xb) = x[(a)+(b)] = x(a\wedge b)$.

Def : a et b sont premiers entre eux si $a\wedge b = 1$ $(a\wedge b\in U(A))$

Thm de Bezout : A principal.

$$a\wedge b = 1 \Longleftrightarrow \exists u,v\in A \text{ t.q } au+bv=1$$

P : $a\wedge b = 1 \Leftrightarrow (a)+(b) = (1) = A \Leftrightarrow 1\in(a)+(b)$.

Corollaire : si $a\wedge b = 1$ et $a\wedge c = 1 \Rightarrow a\wedge bc = 1$

Pr. (voir TD)

Thm. de Gauss.

si a/bc et $a\wedge b = 1 \Rightarrow a/c$

P : Bezout $au+bv=1 \Rightarrow auc+bcv = c \Rightarrow a/c$.

Corollaire (par c) : si $b_1\wedge b_2 = 1$, b_1/a et $b_2/a \Rightarrow b_1b_2/a$

Dém. T.D $b_1u+b_2v=1$, $b_1au+b_2av=a$, $b_1(b_1v)x+b_2(b_2y)x=a$

Déf. Soit $p \in A$ un élément d'un anneau intègre A, $p \neq 0$
p est irréd si :

$\begin{cases} 1) & p \notin U(A) = A^* \\ 2) & \text{s'il existe } a, b \in A \text{ t.q. } p = a.b \text{ alors } a \in A^* \text{ ou } b \in A^* \end{cases}$

Ex : . $A = \mathbb{Z}$, $\pm p$, p premier
. $A = \mathbb{R}[x]$, $x^2 + 1 = f(x)$
$A = \mathbb{C}[x]$
. $A = \mathbb{Q}[x]$, $x^3 - 2 = g(x)$.
$\mathbb{R}[x]$.

Déf 2 . $\neq p$ est irr. si :

$\begin{cases} 1) & p \notin A^* \\ 2) & \text{si } a \mid p \Rightarrow a \in A^* \text{ ou } a \sim p. \end{cases}$

Dém.

PGCD .
. A principal, a, b possèdent un pgcd.
$(a, b) \neq (0, 0)$.

. **corollaire.** A princip. $d = \text{pgcd}(a, b)$
$\begin{cases} \text{alors } \exists x, y \in A \text{ t.q. } ax + by = d. \end{cases}$

Thm. | A principal, $a, b \in A$
π irréd t.q. $\pi \mid ab$ alors $\pi \mid a$ ou $\pi \mid b$

Supp. $\pi \nmid a$
$\lambda = \pi \wedge a = (\pi, a)$ existe, $\lambda \mid \pi \Rightarrow \lambda \in A^*$ ou $\lambda \sim \pi$
$\lambda \sim \pi \Rightarrow \pi \mid a$ contredit $\pi \nmid a$.
donc $\lambda \in A^* \Rightarrow \pi, a$ premiers entre eux (étrangers)

$ax + \pi y = 1$
$(ab)x + \pi(by) = b \Rightarrow \boxed{\pi \mid b}$

Corollaire A principal, π irr.
$\pi \mid a_1 \cdots a_n \Longrightarrow \pi \mid a_i$ pour $i = \overline{1, n}$

Thm

A ann. int. unitaire

(p) max $\Rightarrow$ p irréd

si de plus A est principal

(p) max. $\Leftrightarrow$ p irréd.

Thm 2

A int. unit.

$p \neq 0$

(p) premier $\Rightarrow$ p irr.

$p = ab \in (p)$ premier

Suppp. $a \in (p)$

$p = p \cdot a_1 b$

intégre $\Leftarrow$ $\Rightarrow$ $a_1 \cdot b = 1$, $b \in A^*$ $\longrightarrow$ p irr.

Corollaire

si A est principal $p \neq 0$

(p) max $\Leftrightarrow$ (p) premier $\Leftrightarrow$ p irréd

Anneaux euclidiens (eucli = intgre + st. eucl).

Déf A intègre

A est muni d'1 divi. eucl. (stathme eucl)

$\varphi : A/\{0\} \longrightarrow \mathbb{N}$ t.q.

$\varphi(xy) \geq \varphi(x) \cdot \varphi(y)$

$\forall a, b \in A/\{0\}$, $\exists q, r \in A$ t.q. $a = bq + r$

avec $r = 0$ ou $\varphi(r) < \varphi(b)$.

Ex $\mathbb{Z}$, $\varphi(x) = |x|$

$K(X)$, $\varphi(f) = d^\circ f$.

Thm si A est eucli $\Rightarrow$ A est principal

$\{0\} \neq I$ idéal de A. soit $x \in I$ t.q. $\varphi(x) = \min_{i \in I} \varphi(i)$.

$I = (x)$: pour $a \in I$, $a = x \cdot b + r$, $r \in I$ et

si $r \neq 0$, $\varphi(r) = \varphi(a - xb) < \varphi(x)$!

$r = 0$, $a = xb \in (x)$.

Anneaux factoriels

Déf. Soit A un anneau intègre. On dit que A est un anneau factoriel (a. à factorisation unique) si :

1) $\forall x \in A \setminus (U(A) \cup \{0\})$: x est le produit fini d'éléments irréductibles dans A : $x = p_1 \cdot p_2 \cdots p_k$, p_i irr., $k \geq 1$,

2) si $x = q_1 \cdots q_s$, q_j irr. et $s \geq 1$, une autre écriture de x en produit d'éléments irr. dans A alors $k = s$, et $\forall i = \overline{1,k}$, $\exists! j = \overline{1,k}$ t.q. $q_j \sim p_i$.

Ex. a) $\mathbb{Z}$ est factoriel.

2) ~~$\mathbb{Z}[\xi]$; $\xi = e^{\frac{i2\pi}{5}}$~~

Thm. Tout anneau principal est un anneau factoriel

Preuve : 1) Soit $x \in A \setminus U(A)$, $x \neq 0$.

Supposons que x ne peut être écrit sous la forme produit d'irréductibles dans A.

$\Rightarrow$ x n'est pas irréd. en particulier

$x = a_1 \cdot b_1$ $\quad a_1 \notin U(A)$ et $b_1 \notin U(A)$.

a_1 ou b_1 ne peut être écrit sous forme de produit d'irréductibles. Supposons que c'est a_1.

$x = a_1 \cdot b_1$, $\quad (x) \subsetneq (a_1)$

On applique le même raisonnement avec a_1 ($a_1 \neq 0$, $a_1 \notin U(A)$)

$\exists a_2 \neq 0$, $a_2 \notin U(A)$, $a_2 \neq$ le produit des éléments irréd.,

et $(a_1) \subsetneq (a_2)$, $\quad a_1 = a_2 b_2$.

En procédant de cette manière, on construit $a_3, a_4, \ldots$

$x = a_0$

$(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$

Posons $I = \bigcup_{i \geq 0} (a_i)$.

I est un idéal de A principal, $\exists a \in A$ t.q.

$I = (a)$

On a $a \in I \Rightarrow \exists k \geq 0$, $a \in (a_k)$, donc $(a) \subseteq (a_k)$
et comme $(a_k) \subseteq (a)$, alors $I = (a) = (a_k)$.

En particulier $(a_{k+1}) \subseteq (a_k) \subseteq (a_{k+1})$

donc $(a_k) = (a_{k+1})$, contredit $(a_k) \subsetneq (a_{k+1})$

2) Soit $x \notin U(A) \cup \{0\}$ t.q. $x = \pi_1 \pi_2 \dots \pi_s = \lambda_1 \lambda_2 \dots \lambda_t$.
deux expressions de x en produit d'éléments irréductibles.

si $s = 1 \Rightarrow x$ irréd $\Rightarrow$ l'assertion est vraie

supposons que $s > 1$ (récurrence sur s)

$\pi_1 \mid \lambda_1 \lambda_2 \dots \lambda_t \Rightarrow \pi_1 \mid \lambda_i$ pour un certain $i = \overline{1,t}$

λ_i irréd et $\pi_2 \notin U(A) \Rightarrow \pi_1 \sim \lambda_i$ ($\varepsilon \pi_1 = \lambda_i$, $\varepsilon \in U(A)$)

$$\pi_1 \pi_2 \dots \pi_s = \lambda_1 \lambda_2 \dots \lambda_{i-1} \varepsilon \pi_1 \lambda_{i+1} \dots \lambda_t$$

A intégre $\quad \pi_2 \pi_3 \dots \pi_s = \lambda_1 \lambda_2 \dots \lambda_{i-1} \underbrace{(\varepsilon \lambda_{i+1})}_{\lambda'_{i+1}} \dots \lambda_t$

par hypothèse de récurrence $s - 1 = t - 1$ ($s = t$)
et $\forall i = \overline{2,s}$, $\exists j \in \{1,2,\dots,t\} \setminus \{i\}$ t.q. $\pi_i \sim \lambda_j$.
en remarquant que $\pi_1 \sim \lambda_i$. on obtient le résultat.

Ex. K corps, alors $K[X]$ est factoriel

si $f(x) = a_0 + a_1 X + \dots + a_n X^n$, $a_n \neq 0$.
a_n : le coefficient dominant de f.
si $a_n = 1$, on dit que f est normalisé

On voit : $f(x) = a_n \left(a_n^{-1} a_0 + a_n^{-1} a_1 X + \dots + a_n^{-1} a_{n-1} X^{n-1} + X^n \right)$ non nul non constant

donc $f(x) = a \cdot f_1^* f_2^* \dots f_s^*$

avec $a \in K$ constant et les f_i^* normalisés irréductibles
et cette écriture est unique (à une permutation près).

On retient que :

Euclidien $\Rightarrow$ Principal $\subset$ Factoriel $\subset$ Intégre

$\mathbb{Z}$ et $\mathbb{Z}[i]$ sont factoriels.

Proposition 2.
Soit (a) un idéal propre non nul principal d'un anneau intègre A.
1). si (a) est premier, alors a est irréd.
2) si de plus A est factoriel, alors la réciproque est aussi vraie.

Preuve . 1) $(a) \neq (0) \subsetneq A \Rightarrow a \neq 0$ et $a \notin U(A)$.
si $a = bc$, alors $bc \in (a)$ premier $\Rightarrow b \in (a)$ ou $c \in (a)$
supposons que $b = aq$. Donc $a = a \cdot qc \Rightarrow qc = 1$ et $c \in U(A)$.
2) ($\Leftarrow$) si $bc \in (a)$, alors $a \mid bc \Rightarrow a \mid b$ ou $a \mid c$ c.à.d. $b \in (a)$ ou $c \in (a)$.

Proposition 1.
Soient A factoriel, $a, b, \pi \in A$, π irréd.
si $\pi \mid ab \Longrightarrow \pi \mid a$ ou $\pi \mid b$.

Preuve $\pi \mid ab \Rightarrow \exists k \in A$ t.q. $ab = \pi . k$.
On peut supposer $a \neq 0$, $b \neq 0$, $k \neq 0$.
A factoriel $\Rightarrow$ on peut écrire a et b sous formes de produit d'élts irréd. Comme π apparaît dans le produit d'elts irréd dans l'écriture de $\pi . k$, l'unicité de factorisation entraîne π est associé à un certain irréductible divisant a ou à un certain irréd divisant b. Donc $\pi \mid a$ ou $\pi \mid b$.

Proposition 3 (Lemma de Gauss)
Soient A un anneau factoriel et $\mathbb{Q}$ son corps des fractions
Soit $f(X) \in A[X]$.
si $f(X) = g(X) h(X)$, $g, h \in \mathbb{Q}[X]$ non constants, alors
$f(X) = a(X) b(X)$, $a, b \in A[X]$ non constants.
$f(X)$ irréd dans $A[X]$ ssi $f(X)$ irr. dans $\mathbb{Q}[X]$.

Preuve Pour $c, d \in A$, Les polynômes $g_1 = cg$ et $h_1 = dh \in A[X]$.
$f = gh$ dans $\mathbb{Q}[X]$
$cdf = g_1 \cdot h_1$ dans $A[X]$.
Si p est un irréd. divisant cd. alors modulo (p) on a
$0 = \overline{g_1} \cdot \overline{h_1}$ dans $(A/(p))[X]$.
(p) est premier $\Rightarrow A/(p)$ est intègre $\Rightarrow A/(p)[X]$ est intègre
$\Rightarrow$ p divise tous les coefficients de g_1 ou h_1 au moins. Supposons que c'est g_1. donc $g_1 = p \cdot g_2$
$g_2 \in A[X]$.

$\frac{cd}{p} \cdot f = g_2 \cdot h_2$ dans $A[x]$

en continuant ce procédure, on peut enlever tous les facteurs irréductibles de cd. et on obtient une factorisation de f dans $A[x]$.

Proposition 4

Soit A un anneau factoriel. Soit $\mathcal{P}$ un ensemble des élts irréductibles de A t.q.

(1) Tout élt irréd de A est associé à un élément de $\mathcal{P}$.
(2) Deux éléments de $\mathcal{P}$ ne sont pas associés.

Construction de $\mathcal{P}$

$\mathcal{P}^*$ = l'ens. de tous les élts irréd de A.

Sur $\mathcal{P}^*$: $x \sim y \overset{df}{\Leftrightarrow}$ x et y sont associés

$\sim$ relation d'équivalence

$\mathcal{P}$ est construit en choisissant un seul element dans chaque classe d'équivalence.

$\forall x \in A \setminus \{0\}$ $\quad x = \varepsilon \cdot \prod_{p \in \mathcal{P}} p^{v_p(x)}$ ... (*)

avec $v_p(x) \in \mathbb{N}$, $\varepsilon \in U(A)$ et $v_p(x) = 0$ sauf pour un nombre fini de p.

(*) unique.

Rappel Soient $a_1, a_2, \dots, a_n \in A$, Un pgcd de $a_1, \dots a_n$ est un element $c \in A$ t.q.

1) $c | a_1, \dots, c | a_n$
2) si $d \in A$ t.q. $d | a_1, \dots d | a_n$, alors $d | c$

. Si d et d' sont deux pgcd. de $a_1, \dots, a_n$, alors $d \sim d'$

Lemme Soient A factoriel et $a_1, \dots, a_n \in A$ non tous nuls. Alors $a_1, \dots, a_n$ ont un pgcd.

$a_i = \varepsilon_i \prod_{p \in \mathcal{P}} p^{v_p(a_i)}$, $\varepsilon_i \in U(A)$

Pour $p \in \mathcal{P}$, $v_p = \min \{ v_p(a_1), \dots v_p(a_n) \}$ (= 0 sauf pour un nombre fini de p.)

$c = \prod_{p \in \mathcal{P}} p^{v_p}$ est un pgcd.

Déf : si 1 est un pgcd de $a_1, \dots, a_n$, on dit que $a_1, \dots, a_n$ sont étrangers (ou relativement premiers).

Soit $f(x) = a_0 + a_1 X + \dots + a_n X^n \in A[X] \setminus \{0\}$.

Déf. si $a_0, a_1, \dots, a_n$ sont étrangers, on dit que f est primitif.

Soit c un pgcd de $a_0, a_1, \dots, a_n$

$a_i = k_i \cdot c$

$k_0, \dots, k_n$ sont étrangers

$f(x) = c \cdot \underbrace{(k_0 + k_1 X + \dots + k_n X^n)}_{\text{primitif}}$

Lemme. Soit $f(x) \in A[X]$ non nul. c est un pgcd des coefficients de f. Alors $f = c(f) \cdot f^*$ avec $f^* \in A[X]$ primitif et cette écriture est unique (à multiplication par unités près).

$c(f)$ = le contenu de f.

Ex dans $\mathbb{Z}[X]$:

$4X^5 + 8X^3 + 4X^2 + 12 = 4 \cdot \underbrace{(X^5 + 2X^3 + X^2 + 3)}_{\text{primitif}}$

Thm | Si f et $g \in A[X]$ sont primitifs, alors fg est primitif.

Preuve $f = a_0 + a_1 X + \dots + a_m X^m$, $g = b_0 + b_1 X + \dots + b_n X^n$ } primitifs

· Soit p un élt irréd. de A.

// a_{i_0} = le 1er coeff. de f non divisible par p

// b_{j_0} = " " " g " " " p.

Tous les termes $\sum_{i+j = i_0+j_0} a_i b_j$ sont divisible par p, sauf le terme $a_{i_0} b_{j_0}$ qui n'est pas divisible par p.

$\Rightarrow$ p ne divise pas le $(i_0+j_0)^{\text{ième}}$ terme de fg

On a montré que tout élément irréductible p ne divise pas tous les coefficients de $fg \Rightarrow fg$ est primitif.

Corollaire : 1) Pour $f, g \in A[X]$, $c(fg) \sim c(f) \cdot c(g)$; donc tout facteur d'un polynôme primitif est primitif.

2) Soit $f \in A[X]$ primitif, Q le corps des fractions de A.

Alors f est irréd dans $A[X]$ ssi f irréd dans $Q[X]$.

Dém. exercice.

$$fg = c(f)\cdot \underbrace{f_1}_{\text{prim}} \cdot c(g)\cdot \underbrace{g_1}_{\text{prim}} = c(fg)\cdot \underbrace{h}_{\text{primi}}$$

$$= c(f)\cdot c(g)\cdot \underbrace{f_1 \cdot g_1}_{\text{prim.}}$$

$$\Rightarrow c(fg) \sim c(f)\, c(g).$$

Thm de transfert : Si A est factoriel, alors $A[X]$ est factoriel

Preuve :

1) Soit $f \in A[X]$, $f = c(f)\cdot f_1$ $\quad f_1$ primitif

supposons que f est primitif. Si f n'est pas irréd dans $A[X]$, alors $f = g\cdot h$ $\quad g, h$ primitifs dans $A[X]$ de degrés inférieurs (dc d° f). En continuant on factorise f en produit d'élts irréd. Ces élts irréd sont parmi les polynômes constants et les polynômes primitifs.

2) Soit $f = c_1 c_2 \cdots c_m f_1 \cdots f_n = d_1 \cdots d_r\, g_1 \cdots g_s$

c_i, d_j constants, f_i, g_j irréd. primitifs dans $A[X]$

$c(f) \sim c_1 c_2 \cdots c_m \sim d_1 \cdots d_r$

A factoriel $\Rightarrow m = r$ et $c_i \sim d_j$ $\quad i, j = \overline{1,m}$.

$$f_1 \cdots f_n = g_1 g_2 \cdots g_s \cdot \underbrace{\varepsilon}_{\text{unité dans } A}.$$

Lemme de Gauss : f_i, g_j irréd dans $Q[X]$ et $Q[X]$ est factoriel car principal $\Rightarrow n = s$ et $f_i \sim g_j$, par unité dans Q. Mais si $f_i = \frac{a}{b} g_j$ $\quad a, b$ non nuls de A

$b f_i = a g_j$, f_i, g_j primitifs $\Rightarrow b \mid a$ dans A.

et $\frac{a}{b} \in U(A)$.

Corps commutatifs

1. Introduction

If E is a field, then a subfield of E is a subset of E which is also a field w.r.t. the operations of E.

$\mathbb{Q}$ is a subfield of $\mathbb{R}$

If F is a subfield of E, then we say that E is an extension field (extension) of F.

$\mathbb{R}$ extension of $\mathbb{Q}$.

Example. Consider the set

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{a_0 + a_1\sqrt{2} + a_2(\sqrt{2})^2 + \cdots + a_r(\sqrt{2})^r}{b_0 + b_1\sqrt{2} + \cdots + b_s\sqrt{2}^s},\ a_i, b_j \in \mathbb{Q},\ b_0 + b_1\sqrt{2} + \cdots + b_s\sqrt{2}^s \neq 0 \right\}$$

It is a field containing $\mathbb{Q}$ and $\sqrt{2}$.

- If F is a subfield of $\mathbb{R}$ which contains $\mathbb{Q}$ and $\sqrt{2}$, then $F \supset \mathbb{Q}(\sqrt{2})$. Therefore $\mathbb{Q}(\sqrt{2})$ is the smallest subfield of $\mathbb{R}$ containing $\mathbb{Q}$ and $\sqrt{2}$. $\mathbb{Q}(\sqrt{2})$ is an extension of $\mathbb{Q}$.

Since $\sqrt{2}^2 = 2$, $\sqrt{2}^3 = 2\sqrt{2}, \ldots$

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{\alpha + \beta\sqrt{2}}{\gamma + \delta\sqrt{2}},\ \alpha, \beta, \gamma, \delta \in \mathbb{Q} \right\}.$$

since $(\gamma + \delta\sqrt{2})^{-1} = \dfrac{\gamma^2 - \delta\sqrt{2}}{\gamma^2 - 2\delta^2}$

we see $\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2},\ a, b \in \mathbb{Q} \right\}$.

Generalization

Let E be an extension of a field F. S a set of elements of E, let $\mathcal{C}$ denote the collection of all subfields of E which contain F and S.

Prop. $\bigcap_{G \in \mathcal{C}} G$ is a subfield of E containing F and S, and it is the smallest such field.

$\bigcap_{G \in \mathcal{C}} G$ is denoted by $F(S)$ and is called the field obtained by adjoining S to F.

In the above example $F=\mathbb{Q}$, $E=\mathbb{R}$, $S=\{\sqrt{2}\}$.

$S=\{a_1, a_2, \cdots, a_n\}$, we write $F(a_1, \cdots, a_n)$ instead of $F(\{a_1, \cdots, a_n\})$.

- A field of the form $F(S)$ is an extension of F.
- If E is an extension of F, then $E = F(E)$.

→ Every extension of F can be obtained by adjoining a set of elements to F.

Prop. Let E be an extension of F, S_1, S_2 subsets of E

$$F(S_1 \cup S_2) = F(S_1)(S_2)$$

proof. $F(S_1)(S_2)$ subfield of E containing $F(S_1)$ and S_2.

$\Rightarrow$ $F(S_1)(S_2) \supset F, S_1, S_2 \Longrightarrow F(S_1)(S_2) \supset F, S_1 \cup S_2$.

$\Rightarrow$ $F(S_1)(S_2) \supset F(S_1 \cup S_2)$ ... (1)

put $S = S_1 \cup S_2$

$S_1 \cup S_2 \supset S_1, S_2 \Rightarrow \begin{cases} F(S_1 \cup S_2) \supset F(S_1) \\ F(S_1 \cup S_2) \supset S_2 \end{cases} \Rightarrow F(S_1 \cup S_2) \supset F(S_1)(S_2)$ ... (2)

application

- $F(a_1, \cdots, a_m) = F(a_1, \cdots, a_{n-1})(a_n) = F(a_1, \cdots, a_{n-2})(a_{n-1})(a_n) \cdots$

$a_1, F \xrightarrow{a_1} F(a_1) \xrightarrow{a_2} F(a_1, a_2) \xrightarrow{a_3} \cdots$

Def. An extension of F of the form $F(a)$ is called a simple extension of F.

$$F(a) = \left\{ \frac{f(a)}{g(a)} : f, g \in F[x],\ g(a) \neq 0 \right\}.$$

- A field homomorphism $f: E_1 \to E_2$ is a ring homo. of fields E_1, E_2. ($\Rightarrow f(a^{-1}) = f(a)^{-1}$, $a \neq 0$, $a \in E_1$)

Prop | If $f: E_1 \to E_2$ is a field homo. Then $f \equiv 0$ or f is injective

Proof : exercise. (T.D.)

Def. If E_1 and E_2 are extensions of the same field F, then an F-homo. $f: E_1 \to E_2$ s.t. $f(x)=x$ $\forall x \in F$.
is a homo.

ex. $f: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, $a+b\sqrt{2} \mapsto a-b\sqrt{2}$ is a $\mathbb{Q}$-auto.

$f: \mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ is an $\mathbb{R}$-homo. ($\mathbb{R}$-auto).

Exercise - Determine all the $\mathbb{R}$-auto. of $\mathbb{C}$?
- Show that they form a cyclic group, under "$\circ$"?

Algebraic and transcendental Elements

E is an extension of F. $\alpha \in E$.

Def. α is algebraic over F if there exists a nonzero polynomial $f(x) \in F[x]$ s.t. $f(\alpha)=0$. If α is not algebraic over F, then we say that α is transcendental over F.

Examples 1) $\alpha \in F \Rightarrow \alpha$ is alg. over F. α is a zero of $X-\alpha \in F[X]$.

2) $F=\mathbb{Q}$, $E=\mathbb{C}$, $\alpha_1=\sqrt{2}$, $\alpha_2=\sqrt[3]{7}$, $\alpha_3=\alpha_1+\alpha_2$ are all alg. over $\mathbb{Q}$.

$\alpha_1 \longrightarrow X^2-2$, $\alpha_2 \xrightarrow{\text{zero}} X^3-7$,

$\alpha_3 \longrightarrow X^6-6X^4-14X^3+12X^2-84X+41$.

3) $F=\mathbb{Q}$, $E=\mathbb{C}$, e, π are trans. over $\mathbb{Q}$.
(Hermite, Lindemann)

Theorem of Gelfond-Schneider

Let $\alpha \neq 0, 1$ be algebraic over $\mathbb{Q}$. Let β be alg. over $\mathbb{Q}$, $\beta \notin \mathbb{Q}$. Then α^β is transcendental over $\mathbb{Q}$.

$2^{\sqrt{2}}$ trans. over $\mathbb{Q}$.

($\alpha \in \mathbb{C}$ is alg $\equiv$ alg. over $\mathbb{Q}$ / trans / trans.).

4) F field, $E=F(X)$, X indeterminate over F.
$F(X)$ extension of F (quotient field of $F[X]$)
X is transcendental over F.

$E \supset \alpha$ alg. over F $\longrightarrow$ $\exists f \in F[x]$, $f \neq 0$, s.t. $f(\alpha) = 0$.

$F[x]$ is UFD.

$f = P_1 \cdot P_2 \cdots P_r$, $P_i \in F[x]$ irreducibles

$0 = f(\alpha) = P_1(\alpha) \cdot P_2(\alpha) \cdots P_r(\alpha)$

E integral $\quad p = P_i(\alpha) = 0$ for some $i = \overline{1,r}$.

we may normalize $p = P_i \in F[x]$ to be monic

$\therefore$ p is the unique monic irreducible polynomial in $F[x]$ having α as a zero.

Indeed, if q is another such polynomial $\rightarrow$ p, q are relatively prime, so $\exists\ a, b \in F[x]$ s.t.

$$ap + bq = 1$$

But $0 = a(\alpha)p(\alpha) + b(\alpha) \cdot q(\alpha) = 1$ which is a contradiction.

Prop 1) Let $\alpha \in E$ be alg. over F. Then there exists a unique monic irred polyn. $p \in F[x]$ s.t. $p(\alpha) = 0$.

2) If $f \in F[x]$ be such that $f(\alpha) = 0$. Then f is divisible by p.

notation $p = \operatorname{Irr}(\alpha, x, F) = \operatorname{Irr}_F(\alpha, x)$.

Ex. 1) $\operatorname{Irr}(\sqrt{2}, x, \mathbb{Q}) = x^2 - 2$.

2) $d \in \mathbb{Z}$ not a perfect square ($d \neq x^2$, $x \in \mathbb{Z}$).

$\operatorname{Irr}(\sqrt{d}, x, \mathbb{Q}) = x^2 - d$.

3) $\alpha \in F$, $\quad \operatorname{Irr}(\alpha, x, F) = x - \alpha$.

If E is an ext. of F, then E is an F-vector space w.r.t. $(x, y) \mapsto x + y$ of E

$\alpha \in F$, $x \in E \mapsto \alpha \cdot x$ in E.

The $\dim_F E$ = the degree of E over $F = [E : F] = \deg(E/F)$.

Ex. $\mathbb{Q}(\sqrt{2})$. $\{1, \sqrt{2}\}$ basis of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

$Irr(\sqrt{2}, \mathbb{Q}, X) = X^2 - 2$

we see $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(x^2 - 2)$.

Theorem Let α be alg. over F, $n = \deg(Irr(\alpha, X, F))$. Then

1) $[E : F] = n$. $E = F(\alpha)$.
2) $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ over F.

Proof. ② $\Rightarrow$ ①.

② $F[\alpha]$ the smallest subring of $F(\alpha)$ containing F and α.

$$F[\alpha] = \{ a_0 + a_1\alpha + \cdots + a_m\alpha^m, \ m \geq 0, \ a_i \in F \}$$

show that $$F[\alpha] = \{ b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}, \ b_i \in F \}$$

$$Irr(\alpha, X, F) = X^n + c_{n-1}X^{n-1} + \cdots + c_0.$$

induction on $r \geq n$: $r = n$, $\alpha^n = -c_{n-1}\alpha^{n-1} - \cdots - c_0$

$r > n$, $\alpha^r = \alpha \cdot \alpha^{r-1} = \alpha \cdot (b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1})$

$= b_0\alpha + b_1\alpha^2 + \cdots + b_{n-2}\alpha^{n-1} + b_n(-c_0 - \cdots - c_{n-1}\alpha^{n-1})$

$= b_0' + b_1'\alpha + \cdots + b_{n-1}'\alpha^{n-1}$, $b_i' \in F$.

$$F[\alpha] \subset F(\alpha) \quad \cdots (1)$$

Let $\psi_\alpha : F[X] \to F[\alpha]$ evaluation at α.

$f(X) \mapsto f(\alpha)$

ψ_α surj. homo., with $\ker \psi_\alpha = (Irr(\alpha, X, F))$

$$F[X]/(Irr(\alpha)) \cong F[\alpha]$$

$Irr(\alpha)$ is irred $\to$ $(Irr(\alpha))$ maximal $\to F[X]/(Irr(\alpha))$ field

$\to F[\alpha]$ is a field. $\cdots (2)$

$\Rightarrow$ $F[\alpha] = F(\alpha)$ i.e. $\forall \beta \in F(\alpha)$, $\beta = a_0 1 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$, $a_i \in F$

Uniqueness if $\beta = a_0' \cdot 1 + a_1' \cdot \alpha + \cdots + a_{n-1}'\alpha^{n-1}$

$\Rightarrow (a_0 - a_0') \cdot 1 + (a_1 - a_1')X + \cdots + (a_{n-1} - a_{n-1}')\alpha^{n-1} = 0$

$\Rightarrow \underbrace{(a_0 - a_0') \cdot 1 + \cdots + (a_{n-1} - a_{n-1}')X^{n-1}}_{\text{degree } n-1} \mid \underbrace{Irr(\alpha, X, F)}_{\text{degree } n}$

$\Rightarrow a_0 - a_0' = 0, \dots, a_{n-1} - a_{n-1}' = 0$.

$\{1, \alpha, \dots, \alpha^{n-1}\}$ basis of $F(\alpha)$ over F.

Exa. $\alpha = \sqrt[3]{2}$, $F = \mathbb{Q}$, $E = \mathbb{R}$.

α transcendantal over F

$\psi_\alpha : F[x] \to F[\alpha]$, $\ker \psi = \{0\}$.
$f(x) \mapsto f(\alpha)$

ψ_α induces $F(x) \to F(\alpha)$ F-isomorphism
$q(x) \neq 0$ $\frac{p(x)}{q(x)} \mapsto \frac{p(\alpha)}{q(\alpha)}$

α trans. over F, $\begin{cases} F[\alpha] \subsetneq F(\alpha), \quad F[\alpha] \cong F[x]. \\ F(\alpha) \cong F(x) \\ \deg \alpha \text{ is infinite} \end{cases}$

Def. $E|F$ extension.
E is a finite extension of F (E/F is finite) if $[E:F]$ is finite.

Thm $F(\alpha)/F$ is finite iff α algebraic over F

Ex. 1) Show that $\sqrt{5}$, $\sqrt{11}+1$, $\sqrt[3]{2}+3\sqrt{2}$, $i+1$, are alg. over $\mathbb{Q}$.

2) - show that $\sqrt{2}^{\sqrt{3}}$ is trans. over $\mathbb{Q}$
- Is $\sqrt{2}^{\sqrt{3}}+1$ trans. over $\mathbb{Q}$
$\sqrt{2}^{\sqrt{3}}+\sqrt{2}$ " " ?

3) Let p - an odd prime - and let ξ be a primitive p root of 1. Show that ξ is algebraic over $\mathbb{Q}$?
Show that $\mathrm{Irr}(\xi, \mathbb{Q}, x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.
Describe $\mathbb{Q}(\xi)$.

4) Let α be a complex zero of $X^4 - 5X + 10$
- Describe $\mathbb{Q}(\alpha)$
- compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$

5) Let E/F be an extension.

Def. E is an algebraic extension of F if every $\alpha \in E$ is algebraic over F.

Prop. Let E/F be finite, then E is algebraic over F.

Proof. $[E:F]=n$, $\alpha \in E$

$1, \alpha, \alpha^2, \dots, \alpha^n \in E$ linearly dependent over F since $\dim_F E = n$.

$\Rightarrow \exists\, c_i$ $0 \le i \le n$, not all 0, s.t.

$c_n\alpha^n + c_{n-1}\alpha^{n-1} + \dots + c_1\alpha + c_0 = 0$.

α zero of $f(x) = c_0 + c_1 X + \dots + c_n X^n \in F[x] \neq 0$.

Prop $[E:F] = 1$ iff $F = E$

($\Leftarrow$) Obvious

($\Rightarrow$) $[E:F] = 1$

Thm Let $E \subseteq F \subseteq G$ be three fields. Assume that F/E and G/F are finite ext. Then G/E is finite and $[G:E] = [G:F] \cdot [F:E]$

Proof $\{\alpha_1, \dots, \alpha_n\}$ basis of G over F.

$\{\beta_1, \dots, \beta_m\}$ " " F over E.

$\{\alpha_i \beta_j \quad i=\overline{1,n},\ j=\overline{1,m}\}$ is a basis of G over E.

Corollary. If α_1, α_2 are algebraic over F, then $F(\alpha_1, \alpha_2)$ is finite ext. of F - and is therefore alg. ext.

Proof. $F(\alpha_1)/F$ finite.

α_2 alg over $F \Rightarrow \alpha_2$ alg. over $F(\alpha_1)$

$F \subset \underbrace{F(\alpha_1)}_{\text{finite}} \subset \underbrace{F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2)}_{\text{finite}}$.

Thm $F(\alpha_1, \alpha_2)/F$ finite.

$\Rightarrow$

Corollary. If $\alpha_1, \dots, \alpha_n$ are alg. over F, then $F(\alpha_1, \dots, \alpha_n)/F$ is finite and alg. ext of F.

Proof by induction on n.

Corollary. Let α and β be algebraic over F. Then $\alpha \pm \beta$, $\alpha \cdot \beta$, α/β ($\beta \neq 0$) are alg. over F.

Proof. $F(\alpha, \beta)$ is alg. over F.

Exercises

1) . Show that $X^2 - 3$ is irred in $\mathbb{Q}(\sqrt{2})[X]$
. Compute the degree of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.
. Exhibit a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

2) Let ξ denote the primitive eigth root of 1 given by $\xi = e^{i2\pi/8}$

Show that $(\xi + \xi^{-1})^2 = 2$.

. " $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\xi)$

. Compute $\deg\left(\mathbb{Q}(\xi) \mid \mathbb{Q}(\sqrt{2})\right)$.