CHAPITRE 21

Anneaux

Dans tout ce cours, tous les anneaux considérés seront unitaires et donc la mention d'unitaire sera toujours implicite.

I Idéaux

Définition I.1.

Soit $I \subset A$ une partie de A. on dit que I est un idéal à gauche (resp droite) de A si :

1. $I \leq (A, +)$ i.e. I est un sous-groupe de $(A, +)$
2. $\forall a \in A \; aI \subset I$ (resp $Ia \subset A$)

Si I est un idéal à gauche et à droite, on dit que c'est un idéal bilatère.
On notera alors l'ensemble des ideaux gauches, droite ou bilatère par $Ideal_g(A)$, $Ideal_d(A)$ et $Ideal_b(A)$ respectivement.
Si A est commutatif, alors tout idéal à gauche l'est aussi à droite et sera donc appelé simplement idéal de A.
Dans ce cas, on notera simplement $Ideal(A)$ l'ensemble des ideaux de l'anneau commutatif A.
Finalement, lorsqu'une propriété est vraie dans les trois cas (gauche, droite et bilatère), on dira ideal *gdb* dans l'énoncé. Il faut dans ce cas comprendre qu'il s'agit de trois ennoncés en un.

Exemples : Si $a \in A \; Aa := \{ka \; k \in A\}$ est l'idéal à gauche engendré par a.
Plus généralement, si $S \subset A$ alors l'idéal à gauche engendré par S est $\{\sum_1^n \lambda_i s_i \; n \in \mathbb{N} \;\; \lambda_i \in A \; s_i \in S\}$

Proposition I.2.

1. Soit $I \in Ideal_{gdb}(A)$. Alors $I = A \iff A \cap U(A) \neq \varnothing \iff 1 \in A$ où $U(A)$ désigne le groupe (multiplicatif) des inversibles de A
2. Une intersection quelconque d'idéaux *gdb* est un idéal *gdb*
3. Si $I, J \in Ideal_{gdb}(A)$ alors $I + J \in Ideal_{dgb}(A)$

Exercice I.3.

Soit A un anneau commutatif. Montrer que A corps $\iff Ideal(A) = \{\{0\}, A\}$
En particulier, si A est un corps, alors $Ideal(A \times A) = \{\{(0,0)\}, A \times \{0\}, \{0\} \times A, A \times A\}$

Le reste du cours traitera uniquement les anneaux commutatives.

Définition I.4.

Soit $X \subset A$. Alors $I(X) = \bigcap_{J \in Ideal(A),\ X \subset J} J$ est un idéal de A, appelé idéal engendré par X.
Il s'agit de l'ideal minimum (au sens de l'inclusion) qui contient X.
On le notera aussi $\langle X \rangle$.
Finalement, on dira d'un ideal I qu'il est principal s'il est engendré par un seul element i.e. $I = I(\{a\}) = aA = \{ak,\ k \in A\}$ pour un certain $a \in A$.

1. Idéal engendré

Exemples : $I(\{0\}) = \{0\},\ \ I(\{1\}) = A$

Proposition I.5.

Description interne : Soit $\varnothing \neq X \subset A$. Alors $I(X) = J := \{x \in A,\ \exists n \in \mathbb{N}\ \exists (x_1, \dots, x_n) \in X^p\ \exists (a_1, \dots, a_n) \in A^n\ \ x = \sum_1^n a_i x_i\}$

En effet, $J \in Ideal(A),\ X \subset J$ est clair et de plus $\forall I \in Ideal(A)\ X \subset I \Longrightarrow J \subset I$ d'où le résultat

Remarque : $I(X) = A \Longleftrightarrow \exists n \in \mathbb{N}\ \exists (x_1, \dots, x_n) \in X^p\ \exists (a_1, \dots, a_n) \in A^n\ \ \sum_1^n a_i x_i = 1$

2. Idéal et morphisme

Définition I.6.

On dit que $f : A \longrightarrow B$ un morphisme d'anneau (qu'on notera désormais $Hom_{anneau}(A, B)$) si

- $\forall (a, b) \in A^2\ f(a + b) = f(a) + f(b)$
- $\forall (a, b) \in A^2\ f(ab) = f(a)f(b)$
- $f(1_A) = 1_B$

Proposition I.7.

Soit $f \in Hom_{anneau}(A, B)$. Alors :

1. $Im(f) = f(A)$ est un sous-anneau de B
2. $\forall I \in Ideal(A)\ f(I) \in Ideal(Im(f))$. En particulier, si f est surjectif, alors $\forall I \in Ideal(A)\ f(I) \in Ideal(B)$
3. $\forall I \in Ideal(B)\ f^{-1}(I) \in Ideal(A)$. En particulier, $Ker(f) := f^{-1}(\{0_B\}) \in Ideal(A)$

Preuve :

1. La stabilité par addition et multiplication est claire. $1_B \in Im(f)$ est vraie car $f(1_A) = 1_B$
2. $f(I) \leq (B, +)$ est directe. Soit $a \in A$ et $i \in I$ alors $f(a)f(i) = f(ai) \in f(I)$
3. $f^{-1}(I) \leq (A, +)$ est directe. Soit $a \in A\ i \in f^{-1}(I)$. Alors $f(ai) = f(a)f(i) \in I$ et donc $ai \in f^{-1}(I)$

Définition I.8.

Soit $I \in Ideal(A)$

- On dit que I est premier si $\forall x, y \in A\ xy \in I \Longrightarrow x \in I$ ou $y \in I$.
- On dit que I est maximal si $I \neq A$ et $\forall J \in Ideal(A)\ I \subset J \Longrightarrow J \in \{I, A\}$. On verra que maximal implique premier.
- On dit que I est radical si $\forall x \in A\ \forall n \in \mathbb{N}^*\ x^n \in I \Longrightarrow x \in I$. En particulier, tout idéal premier est radical.

Exercice I.9.

1. Soit $I \in Ideal(A)$ tel que $I \neq A$. Montrer que I maximal implique que I est premier. A-t-on toujours l'inverse ?
2. Trouver les ideaux premiers de $\mathbb{Z}$
3. Trouver les ideaux maximaux de $\mathbb{Z}$
4. Montrer que $\{0\}$ est :
   - Maximal $\Longleftrightarrow$ A est un corps
   - Premier $\Longleftrightarrow$ A est intègre
   - Radical $\Longleftrightarrow$ A est réduit i.e. le seul élément nilpotent de A est 0

   On généralisera ces résultat à d'autres ideaux plus tard.
5. On admettera dans cette question le théorème de Krull (voir l'appendix). Soit A un anneau. On dit que A est local $\Longleftrightarrow$ A possède un unique idéal maximal. Montrer que A est local $\Longleftrightarrow$ $J := \{x \in A,\ x \notin U(A)\}$ est un idéal. ($U(A)$ désigne le groupe multiplicatif des inversibles de A).
   Remarquer au passage que, dans ce cas, l'unique idéal maximal de A est exactement J.
6. Exemple : Soit $\mathbb{K}$ un corps et $A \subset \mathbb{K}$ un sous-anneau de $\mathbb{K}$ qui vérifie $\forall x \in \mathbb{K}\backslash\{0\}\ x \in A$ ou $x^{-1} \in A$. Montrer que A est radical.

II Divisibilité

On suppose dans cette partie que A est intègre

Définition II.1.

Soit $(a, b) \in A^2$. On dit que a divise b et on le note a|b si $\exists c \in A\ b = ac$ ou, équivalent, $\langle b\rangle \subset \langle a\rangle$. On note alors $Div(a)$ l'ensemble des diviseurs de a.
On dit alors que a et b sont associés si $a|b$ et $b|a$ ou, ce qui lui est équivalent, que $\exists u \in U(A)\ a = ub$. On le notera $a \sim b$.
On notera de plus $\overline{a} := \{c \in A,\ a \sim c\}$

Preuve : Si $a = ub$ avec $u \in U(A)$ alors $b = u^{-1}a$ et donc $a|b$ et $b|a$
Inversement, si $b = ac$ et $a = bd$ alors $acd = a$. A étant intègre, on déduit que soit $a = 0$ et donc $b = 0$, soit $cd = 1$ et donc $c, d \in U(A)$.
Exemple : $Div(0) = A$ et $Div(1) = U(A)$

Proposition II.2.

1. $\sim$ est une relation d'équivalence
2. $\langle a\rangle = \langle b\rangle \iff \overline{a} = \overline{b}$. En particulier, on pourra écrire $\langle\overline{a}\rangle$ pour dire aussi bien l'idéal engendré par a que par sa classe.
3. La relation de division passe au quotient i.e. $a|b \iff \forall x \in \overline{a}\ \forall y \in \overline{b}\ x|y$. On pourra alors écrire $\overline{a}|\overline{b}$ pour signifier que ce qui précède est vrai.
4. La multiplication passe au quotient i.e. $\overline{ab} = \overline{a}\cdot\overline{b}$
5. La division est une relation d'ordre sur $A/\sim$

1. - $a \sim a$ car $a = 1\cdot a$.
   - Si $b = ua$ avec $u \in U(A)$ alors $a = u^{-1}b$ et $u^{-1} \in U(A)$
   - Si $b = ua$ et $c = vb$ avec $u, v \in U(A)$ alors $c = vua$ et $vu \in U(A)$
2. $\langle a\rangle = \langle b\rangle \iff \langle a\rangle \subset \langle b\rangle$ et $\langle b\rangle \subset \langle a\rangle \iff b|a$ et $a|b \iff a \sim b \iff \overline{a} = \overline{b}$
3. $\Longleftarrow$: clair
   $\Longrightarrow$: Supposons $b = ac$ et soit $u, v \in U(A)$ alors $vb = vau^{-1}(ua)$ et donc $au|bv$
4. $\overline{a}\overline{b} = aU(A)bU(A) = abU(A)^2 \underset{U(A)\text{ groupe}}{=} abU(A) = \overline{ab}$
5. Direct en se rappelant que $a|b$ et $b|a \iff a \sim b$ et en utilisant ce qui précède

Définition II.3.

Soit $(a, b) \in A^2\backslash\{(0, 0)\}$. On dit que $d \in A$ est un pgcd de (a, b) si $\forall c \in A\ c|a$ et $c|b \iff c|d$. Le pgcd n'existe pas toujours. Toutefois, s'il existe, alors l'ensemble des pgcd est exactement la classe d'un d'eux. En particulier, le pgcd, s'il existe, est unique à associé près et on peut donc écrire sans ambiguité $\overline{d} = \overline{a}\wedge\overline{b} = a\wedge b$.

Preuve : Il est clair que si d est un pgcd alors ud où $u \in U(A)$ l'est aussi. Réciproquement, si d et d' sont deux pgcd alors $d|d'$ et $d'|d$ et donc $d \sim d'$

Remarque : Même si un pgcd existe on a, en général, pas forcément de relation de Bezout

Définition II.4.

$p \in A\backslash\{0\}$ est dit irréductible si $p \notin U(A)$ et $Div(p) = U(A)\bigcup\overline{p}$.
Remarquer que la notion d'irréductible passe au quotient i.e. qu'un élément p est irréductible $\iff$ tout élément de $\overline{p}$ l'est. On pourra donc dire $\overline{p}$ est irréductible.
On dit que $p \neq 0$ est premier si $p \notin U(A)$ et $\forall(a, b) \in A^2\ p|ab \iff (p|a$ ou $p|b)$. De même, la notion de primalité passe au quotient et donc on pourra dire que $\overline{p}$ est premier.

Proposition II.5.

Tout élément premier est irréductible. La réciproque par contre n'est pas toujours vraie. On verra dans la suite qu'elle est vraie dans les anneaux principaux par exemple (et, plus généralement, dans les anneaux factoriels).

Preuve : Soit p premier et écrivons $p = ab$. En particulier, $p|ab$ et donc $p|a$ ou $p|b$, Disons sans perte de généralité que $p|a$. On a alors de même que $a|p$ et donc $a \sim p$ i.e. $p = au$ avec $u \in U$. Or, $p \neq 0$ et A est intègre d'où $b = u \in U(A)$.

III Anneaux principaux

1. Généralités

Définition III.1.

On dit que A est principal lorsqu'il est intègre et que tout idéal de A est principal.

Exemple : $\mathbb{Z}$, $\mathbb{K}[X]$: il suffit de faire des divisions euclidiennes sur des elements minimaux (en valeur absolue ou en degré)
⚠$\mathbb{Z}[X]$ n'est pas principal car $I = I(\{2, X\})$ n'est pas principal. En effet, si $I = \langle a\rangle$ alors $a|2$ et donc $a \in \{\pm 1, \pm 2\}$ et aucune de ces 4 possibilités n'est vraie.

2. Arithmétique des anneaux principaux

Dans tout ce qui suit A est principal

Théorème III.2.

Soit $(a, b) \in A^2\backslash\{(0, 0)\}$. Alors (a, b) possède un pgcd d. De plus, e est un pgcd de $(a, b) \iff e \in \overline{d} \iff \langle e\rangle = \langle a\rangle + \langle b\rangle$ En particulier, on a une relation de Bezout et $\overline{a} \wedge \overline{b} \subset U(A) \iff \overline{a} \wedge \overline{b} = U(A) \iff \exists (u, v) \in A^2,\ au + bv = 1$. On note dans ce cas, pour simplifier, $a \wedge b = 1$ et on dit que a et b sont premiers entre eux.

- Existence : A étant principal, on peut considérer d tel que $\langle d\rangle = \langle a\rangle + \langle b\rangle$. On a alors $d|a$ et $d|b$ et une relation de bezout $d = au + bv$ avec $u, v \in A$. De plus, si $c|a$ et $c|b$ alors $c|au + bv = d$ et donc d est bien un pgdc.
- e est un pgcd de $(a, b) \iff e \in \overline{d} \iff \langle e\rangle = \langle a\rangle + \langle b\rangle$: On sait que l'ensemble des pgdc de (a, b) est exactement $\overline{d}$ et que l'ensemble des $e \in A$ tel que $\langle e\rangle = \langle d\rangle$ est aussi exactement $\overline{d}$ d'où l'équivalence
- $\overline{a} \wedge \overline{b} \subset U(A) \implies \overline{a} \wedge \overline{b} = U(A)$: La seule classe qui rencontre $U(A)$ est $U(A)$ d'où l'égalité
- $\overline{a} \wedge \overline{b} = U(A) \iff \exists (u, v) \in A^2,\ au + bv = 1$: $\overline{a} \wedge \overline{b} = U(A) \iff \overline{a} \wedge \overline{b} = \overline{1} \iff A = \langle 1\rangle = \langle a\rangle + \langle b\rangle \iff 1 \in \langle a\rangle + \langle b\rangle \iff \exists (u, v) \in A^2,\ au + bv = 1$

Proposition III.3.

Soit $(a, b) \in A^2\backslash\{(0, 0)\}$, $c \in A$ tel que $(a, c) \neq (0, 0)$ et $\lambda \in A\backslash\{0\}$

1. $\lambda a \wedge \lambda b = \lambda \cdot (a \wedge b)$
2. Soit $d \in a \wedge b$. Alors $\frac{a}{d} \wedge \frac{b}{d} = 1$
3. $(a \wedge b = 1$ et $a \wedge c = 1) \iff a \wedge bc = 1$
4. Gauß : Si $a|bc$ et $a \wedge b = 1$ alors $a|c$

Preuve :

1. Remarquons d'abord que tout élement de $\lambda a \wedge \lambda b$ est un multiple de λ. Ceci car, $\lambda|\lambda a$ et $\lambda|\lambda b$. On pourra donc écrire, pour un tel élement (et par intégrité), $\frac{d}{\lambda}$ sans souci.

$$d \in \lambda a \wedge \lambda b \iff \langle d\rangle = \langle \lambda a, \lambda b\rangle \iff \lambda\langle \frac{d}{\lambda}\rangle = \lambda\langle a, b\rangle \iff \langle \frac{d}{\lambda}\rangle = \langle a, b\rangle \iff \frac{d}{\lambda} \in a \wedge b$$

2. Par ce qui précède $\frac{a}{d} \wedge \frac{b}{d} = \frac{1}{d}a \wedge b = \frac{1}{d}\overline{d} = \overline{1}$

3. $\Longleftarrow$: clair.
   $\Longrightarrow$: Soit $d \in a \wedge bc$. Alors $d|ac$, $d|ab$ et $d|bc$ et donc $\overline{d}|ac \wedge bc = c(a \wedge b) = \overline{c}$ et de même $d|b$. Finalement, ceci donne que $\overline{d}|a \wedge b = \overline{1}$ et donc $a \wedge bc = 1$
4. Ecrivons $au + bv = 1$ et $bc = ax$. Alors $c = acu + bcv = acu + axv$ et donc $a|c$

3. Element irréductible

A est toujours supposé principal

Proposition III.4.

Soit $(a, p) \in (A\backslash\{0\})^2$ avec p irréductible.

1. soit $p|a$ soit $p \wedge a = 1$. En particulier, si a aussi est irréductible, alors soit $p \sim a$ soit $p \wedge a = 1$.
2. p est premier

Preuve :

1. Supposons que $p \nmid a$. Soit alors $d \in p \wedge a$. $d \in Div(p)$ et $d \notin \overline{p}$ et donc $d \in U(A)$ i.e. $p \wedge a = 1$
2. Supposons $p|ab$. Si $p|a$ alors c'est bon sinon $p \wedge a = 1$ et donc, par Gauß, $p|b$.

Théorème III.5.

Soit $a \in A\backslash\{0\}$. Alors $\exists u \in U(A)\ \exists n \in \mathbb{N}\ \exists(p_1, \dots, p_n)$ irréductibles tel que $a = up_1 \dots p_n$. De plus, cette écriture est unique au sens suivant : si $a = u'p'_1 \dots p'_m$ avec les même conditions qu'avant alors $n = m$ et, quitte à réordonner les p'_i, on a $\forall i\ p_i \sim p'_i$.
En d'autres mots, $\exists n \in \mathbb{N}\ \exists \overline{p}_1, \dots, \overline{p}_n$ irréductibles tel que $\overline{a} = \overline{p}_1 \dots \overline{p}_n$ et cette écriture est unique à permutation près.

On ne fera que la preuve d'unicité ici. Pour celle de l'existence, voir la partie complément cas général.
On fera remarquer au passage que pour des anneaux qu'on controle bien tel que $\mathbb{Z}$ ou $\mathbb{K}[X]$ (ou, plus généralement, pour des anneaux euclidiens) une preuve très similaire mais formulée plus facilement peut être fait par récurrence, ici sur la valeur absolue ou degré (et, plus généralement, sur le stathme euclidien).
On fera une récurrence forte sur le nombre d'irréductibles dans une écriture minimale en taille de a, le cas $n = 0 \Longleftrightarrow a \in U(A)$ étant trivial. Ecrivons $a = up_1 \dots p_n$ et $a = u'p'_1 \dots p'_m$. Notre premier but est de montrer que l'un des $p'_i \sim p_1$. Cela vient directement de la primalité de p_1. En effet, $p_1|u'p'_1 \dots p'_m$ et donc $p_1|u'$ ou l'un des p'_i. Le premier cas étant impossible, on a le résultat voulu.
Quitte à réordonner les p'_i et changer le u', on peut supposer que $p_1 = p'_1$ et donc $\dfrac{a}{p_1} = up_2 \dots p_n = u'p'_2 \dots p'_m$. Ceci donne, par récurrence, que $n = m$ puis que, à ordre près, $\forall j\ p_j \sim p'_j$ D'où le résultat.
Application : $\mathbb{Z}$ et $\mathbb{K}[X]$.

4. Complément cas général

Définition III.6.

A est dit noethérien si tout suite croissante d'idéaux est stationnaire.
Ceci est équivalent à dire que tout idéal est finiment engendré et donc, en particulier, tout anneau principal est noethérien.

Preuve : $\Longrightarrow$: Supposons qu'un idéal I ne soit pas finiment engendré. On peut alors construire une suite (a_n) d'élements de I tel que $a_0 \in I$ quelconque et $a_{n+1} \notin I_n := \langle a_0, \dots, a_n \rangle$. On a alors une suite

strictement croissante d'idéaux ce qui contredit notre hypothèse.
$\Longleftarrow$: Prenons une suite croissante d'ideaux $I_0 \subset I_1 \dots$ et posons $I = \bigcup_{k\in\mathbb{N}} I_k$. Il est aisé de vérifier que I est un idéal et donc, par hypothèse, $I = \langle a_1 \dots a_n \rangle$. On a alors $\forall i\ a_i \in I = \bigcup_{k\in\mathbb{N}} I_k$ et donc $\forall i\ a_i \in I_{k_i}$ pour un certain k_i. En posant $k = max(k_1, \dots, k_n)$, on a alors $I \subset I_k$ et donc la suite stationne.
Preuve :
Faisons maintenant la preuve de l'existence d'une factorisation de $a \in A\backslash\{0\}$, par l'absurde.
a n'est ni inversible ni irréductible. On peut alors écrire $a = b_1 b_2$ avec les deux non inversibles et donc, en particulier, vérifient de plus $b_1 \not\sim a$ et $b_2 \not\sim a$. Si les deux sont factorisables comme voulu alors on obtient une contradiction. Ainsi, sans perte de généralité, on peut dire que b_1 n'est pas factorisable. Comme précédement, on peut donc écrire $b_1 = c_1 c_2$ avec les deux non irréductibles et donc tous deux non associés à b_1. On continue ainsi de suite cette construction. On obtient donc à chaque étape une élément $a_n | a_{n-1}$ qui ne se factorise pas. Posons alors $I_n = \langle a_n \rangle$. Il est clair que c'est une suite croissante d'idéaux et que de plus elle ne stationne pas car elle strictement croissante $a_n \not\sim a_{n-1}$ d'où notre contradiction.

5. Ecriture d'un élément

Notons $\mathcal{P}$ un choix d'un représentant pour chaque classe d'élément irréductible.
Exemple : $\mathbb{Z} \longrightarrow \mathcal{P} = \{2, 3, ...\}$
$\mathbb{K}[X] \longrightarrow \mathcal{P} = \{P \text{ irréductible unitaire}\}$
Ecriture :

Proposition III.7.

Soit $0 \neq a \in A$.

1. Il existe un unique $u \in U(A)$ et une unique famille $(\alpha_p)_{p\in\mathcal{P}} \in \mathbb{N}^{(\mathcal{P})}$ à support fini tel $a = u \prod_{p\in\mathcal{P}} p^{\alpha_p}$. On nomera le coefficient α_p la valuation $p-$adique de a et on le notera $v_p(a) = \alpha_p$.
2. Soit $b \in A\backslash\{0\}$. Alors $\forall p \in \mathcal{P}\ v_p(ab) = v_p(a) + v_p(b)$. En particulier,
$$a|b \Longleftrightarrow \forall p \in \mathcal{P}\ v_p(a) \leq v_p(b)$$
3. Maintenant qu'on a fait un choix de représentant, on peut se passer de la classe du pgcd à un représentant normalisé. On a alors, en gardant les même notations que ci-dessus :
$$a \wedge b = \prod_{p\in\mathcal{P}} p^{min(\alpha_p,\beta_p)} \text{ et } a \vee b = \prod_{p\in\mathcal{P}} p^{max(\alpha_p,\beta_p)}$$
4. Notons $d(a)$ le nombre de diviseurs normalisés de a (ou, equivalent, le nombre de classes qui divisent $\overline{a}$). Alors
$$d(n) = \prod_{p\in\mathcal{P}} (1 + \alpha_p)$$

Preuve :

1. Direct de ce qui précède en remarquant que l'inversible u est fixé vu que les irréductibles sont désormais normalisés (i.e. qu'on a pris des représentants)
2. Ecrivons $a = u \prod_{p\in\mathcal{P}} p^{\alpha_p}$ et $b = v \prod_{p\in\mathcal{P}} p^{\beta_p}$
   - $ab = uv \prod_{p\in\mathcal{P}} p^{\alpha_p+\beta_p}$ et donc $v_p(ab) + v_p(a) + v_p(b)$.
   - $\Longrightarrow$: direct ce ce qui précède
   - $\Longleftarrow$: $b = ac$ avec $c = vu^{-1} \prod_{p\in\mathcal{P}} p^{\beta_p-\alpha_p}$

3. On fera la preuve uniquement pour le pgdc. Pour le ppcm elle est similaire. Posons $A = \prod_{p\in\mathcal{P}} p^{min(\alpha_p,\beta_p)}$.
   Il est clair par ce qui précède que $A|a$ et $A|b$. Soit d (non nul) tel que $d|a$ et $d|b$. Alors $\forall p \in P\ v_p(d) \leq v_p(a)$ et $v_p(d) \leq v_p(b)$ d'où $\forall p \in P\ v_p(d) \leq min(v_p(a), v_p(b))$ et donc $d|A$.
4. Par ce qui précède,

$$d(n) = |\{(\beta_p)_{p\in\mathcal{P}} \in \mathbb{N}^{(\mathcal{P})}\ \forall p \in \mathcal{P}\ \beta_p \leq \alpha_p\}| = \prod_{p\in\mathcal{P}} (1+\alpha_p)$$

Exercice III.8.

Soit $a, n \geq 2$.

1. Montrer que si $a^n - 1$ est premier alors n est premier
2. Montrer que si $a^n + 1$ est premier, alors n est une puissance de 2.
3. Montrer qu'il existe une infinité de nombres premiers congrus à -1 modulo 4.

6. Ideaux

A est toujours supposé principal.
Commencons par les cas triviaux

Proposition III.9.

1. $\{0\}$ est maximal que si A est un corps. A n'est pas maximal par définition.
2. $\{0\}$ est premier (A est intègre). A est premier.
3. $\{0\}$ est radical (A est intègre). A est radical.

Proposition III.10.

Le Soit $\{0\} \neq I = \langle a\rangle \neq A$ un ideal non trivial de A (equivalent à $a \notin \{0\} \cup U(A)$). On a alors $a = u\prod_1^n p_i^{\alpha_i}$ avec $u \in U(A), \alpha_i \geq 1, n \geq 1$ et les p_i sont irréductibles non associés deux à deux. Alors :

1. I est maximal $\iff n = 1$ et $\alpha_1 = 1$
2. I est premier $\iff n = 1$ et $\alpha_1 = 1$
3. I est radical $\iff \forall i\ \alpha_i = 1$

En particulier, les ideaux non triviaux principaux et maximaux coincident.

1. $\Longrightarrow$: $I \subset \langle p_1\rangle \neq A$ d'où le résultat
   $\Longleftarrow$: Supposons $I \subset J \neq A$ avec $J = (b)$ un ideal. Alors $b|p_1$ et donc b est soit inversible (impossible), soit $b \sim p_1$ auquel cas $I = J$ d'où le résultat.
2. $\Longleftarrow$: Direct vu qu'un ideal maximal est aussi premier
   $\Longrightarrow$: On a $a = u\prod_1^n p_i^{\alpha_i} \in I$ d'où, par primalité, soit $u \in I$ soit l'un des $p_i \in I$. Le premier cas étant impossible, on a alors, quitte à réordonner les p_i, que $p_1 \in I$. Ainsi $a = u\prod_1^n p_i^{\alpha_i} | p_1$ et donc $n = 1$ et $\alpha_1 = 1$.
3. $\Longrightarrow$: Pour $m = max(\alpha_i) \geq 1$ on a $(p_1 \dots p_n)^m \in I$ et donc, par radicalité, $p_1 \dots p_n \in I$ d'où $a = u\prod_1^n p_i^{\alpha_i} | p_1 \dots p_n$ et donc $\forall i\ \alpha_i = 1$ ($\alpha_i \geq 1$)

$\Longleftarrow$: Prenons $b \in A$ et $n \geq 1$ tel que $b^n \in I$. Alors, $\forall i\ v_{p_i}(b^n) = nv_{p_i}(b) \geq v_{p_i}(a) = \alpha_i = 1$ et donc $\forall i\ v_{p_i}(b) \geq 1$ d'où $a|b$

IV Compléments (HP)

Dans tout ce qui suit, A est un anneau commutatif (unitaire) quelconque.

1. Quotient

Rappel :
Soit $I \leq (A, +)$. La théorie des groupe nous donne que $(A/I, +)$ a une structure naturelle de groupe. En fait, si on suppose $I \in Ideal(A)$ avec $I \neq A$, alors on a même mieux.

Proposition IV.1.

Soit I un idéal strict de A. Alors $(A/I, +, \cdot)$ possède une structure naturelle d'anneau quotient définie par $(a+I)+(b+I) = (a+b)+I$ $(\overline{a}+\overline{b} = \overline{a+b})$ et $(a+I)(b+I) = ab+I$ $(\overline{a}\cdot\overline{b} = \overline{ab})$. Cette structure fait de la projection naturelle $\pi : A \to A/I$ désormais un morphisme d'anneaux surjectif (de noyaux I).

Preuve : : Similaire aux groupes quotients : vérifier les axiomes d'un anneau en montrant l'indépendance des lois de leurs représentants. Le fait que ce soit un morphisme d'anneaux vient directement de la forme des nouvelles lois.

Théorème IV.2.

1. (1er théorème d'isomorphisme) Soit $\phi : A \to B$ un morphisme d'anneaux. Alors ϕ induit un morphisme d'anneaux injectif $\overline{\phi} : A/ker(f) \to B$ qui vérifie de plus $\phi = \overline{\phi} \circ \pi$. En particulier, $A/ker(f) \simeq Im(f)$
2. Plus généralement si $I \in Ideal(A),\ I \subset Ker(f)$ alors ϕ induit un morphisme d'anneaux $\overline{\phi} : A/I \to B$ avec toujours $\phi = \overline{\phi} \circ \pi$ et $Ker(\overline{\phi}) = \pi(Ker(f)) = \overline{Ker(f)} = \{x + I,\ x \in Ker(f)\} = Ker(f)/I$
3. En particulier, en prenant $I, J \in Ideal(A)$ avec $J \subset I \neq A$, on obtient un morphisme d'anneaux canonique $\overline{\pi} : A/J \to A/I$ qui envoie $x + J$ à $x + I$ et de noyaux I/J. Ceci fournit en particulier que $(A/J)/(I/J) \simeq A/I$

1. Similaire aux groupes quotients

2. Similaire aux groupes quotients

3. $\pi : A \to A/I$ vérifier $J \subset I = Ker(\pi)$ et donc on obtient $\overline{\pi} : A/J \to A/I$. On obtient donc finalement par le 1er théorème d'isomorphisme que $Im(f) = A/J \simeq (A/J)/ker(\overline{\pi}) = (A/J)/(I/J)$

Proposition IV.3.

Soit A un anneau et I un idéal strict de A. Plusieurs propriétés de I se lisent sur l'anneau quotient A/I. En voici quelques exemples :

1. A/I est un corps $\iff$ I est maximal
2. A/I est intègre $\iff$ I est premier
3. A/I est réduit $\iff$ I est radical

Remarquons qu'avec cette caractérisation il est aisé de voir que maximal $\implies$ premier $\implies$ radical.

1. I maximal $\iff \forall a \notin I\ \langle a\rangle + I = A \iff \forall a \notin I\ \exists u \in A\ \exists i \in I\ au + i = 1 \iff \forall a \notin I\ \exists u \in A\ \overline{au} = \overline{1} \iff \forall a \notin I\ \overline{a} \in U(A/I) \iff U(A/I) = A/I\backslash\{\overline{0}\} \iff A/I$ corps

2. I premier $\iff (\forall a, b \in A\ ab \in I \implies a \in I$ ou $b \in I) \iff (\forall a, b \in A\ \overline{ab} = 0 \implies \overline{a} = 0$ ou $\overline{b} = 0) \iff A/I$ intègre

3. I radical $\iff (\forall x \in A\ \forall n \geq 1\ x^n \in I \implies x \in I) \iff (\forall x \in A\ \forall n \geq 1\ \overline{x^n} = 0 \implies \overline{x} = 0) \iff A/I$ réduit

Afin de mieux étudier A/I, on aimerait mieux comprendre ses idéaux. On a alors la proposition suivante qui fournit un dictionnaire de ces ideaux

Proposition IV.4.

Posons $J(A, I) = \{J \in Ideal(A),\ I \subset J\}$. Alors $\tilde{\pi} := \pi\Big|_{J(A,I)}^{Ideal(A/I)}$ est une bijection croissante (pour l'inclusion) d'inverse $\tilde{\pi}^{-1} := \pi^{-1}\Big|_{Ideal(A/I)}^{J(A,I)}$ (π^{-1} est l'application image réciproque induite par π).

Preuve :

- π étant surjective, elle envoie bien $Ideal(A)$ vers $Ideal(A/I)$ et donc, en particulier, $J(A, I)$ vers $Ideal(A/I)$. Ainsi, $\tilde{\pi}$ est bien définie.
- π^{-1} envoie bien tout idéal de A/I vers un idéal de A contenant $Ker(\pi) = I$ et donc π^{-1} est bien définie de $Ideal(A/I)$ vers $J(A, I)$
- La croissance pour l'inclusion est directe
- On sait que, en général et même pour tout application f, $f \circ f^{-1}(X) = X \cap Im(f)$. Ainsi, π étant surjective, on a que $\tilde{\pi} \circ \tilde{\pi}^{-1} = \mathrm{Id}$
- Soit $\varnothing \neq X \subset A$. Alors il est aisé de vérifier que $\pi^{-1} \circ \pi(X) = X + Ker(\pi) = X + I$. En particulier, pour $J \in J(A, I)$, $\tilde{\pi}^{-1} \circ \tilde{\pi}(J) = \pi^{-1} \circ \pi(J) = J + I = J$

On ajoutera un dernier théorème parfois pratique, qui permet de mieux comprendre la structure d'anneau quotient dans certain cas

Théorème IV.5.

(Théorème chinois) Soit $I, J \in Ideal(A)$ des ideaux stricts de A étrangers i.e. tel que $I+J=A$. Alors :

1. $IJ := \langle \{ij, i \in I\ j \in J\} \rangle = I \cap J$ (remarquer qu'en general on a simplement $IJ \subset I \cap J$)
2. $$\phi : \begin{cases} A/(I \cap J) & \longrightarrow A/I \times A/J \\ x + I \cap J & \mapsto (x+I, x+J) \end{cases}$$
   est un isomorphisme d'anneaux.
3. La propriété se généralise aisement par récurrence à n ideaux 2 à 2 étrangers entre eux.
4. Supposons désormais A principal (par exemple $A = \mathbb{Z}$). Alors :
   - $I = (a), J = (b)$
   - La condition $I + J = A$ est équivalente à $a \wedge b = 1$
   - La condition $I, J \neq A$ est équivalente à $a, b \notin U(A)$
   - Le premier résultat fournit que $(a) \cap (b) = (ab)$
   - On obtient finalement un isomorphisme $\phi : A/abA \to A/aA \times A/bA$
   - Plus intéréssant : En écrivant $a = u \prod_1^n p_i^{\alpha_i}$ où $u \in U(A)$, $\forall i\ \alpha_i \geq 1$ et les p_i sont des irréductibles deux à deux non associés alors $A/aA \simeq \prod_1^n A/p_i^{\alpha_i}A$

Preuve :
On notera, pour distinguer les projections quand nécéssaire, $\pi_K : A \to A/K$ la surjection canonique si $K \in Ideal(A)$.

1. $IJ \subset I \cap J$ est clair
   Soit $x \in I \cap J$ et écrivons $i + j = 1$ avec $i \in I\ j \in J$. Alors $x = xi + xj \in IJ$
2. - $I \cap J \subset I, J$ et donc ϕ est bien définie
   - Soit $x \in A$ tel que $\pi_{I \cap J}(x) \in Ker(\phi)$, alors $x \in I$ et $x \in J$ et donc $x \in I \cap J$ d'où ϕ est injectif. Remarquer au passage que l'injectivité et bonne définition de ϕ ne relèvent par de l'hypothèse $I + J = A$.
   - Ecrivons $i + j = 1$ avec $i \in I\ j \in J$ et prenons $a, b \in A$. Alors, en posant $x = bi + aj = b(1-j) + a(1-i)$, on a $\phi(x) = (\overline{a}, \overline{b})$ et donc ϕ est surjectif.
3. Récurrence directe
4. Application directe du théorème

2. Appendix

Théorème IV.6.

(Krull) Soit A un anneau et $I \in Ideal(A)$ un ideal strict de A. Alors il existe un ideal maximal $\mathcal{M} \in Ideal(A)$ qui vérifie $I \subset \mathcal{M}$

La démonstration dans le cas noetherien n'est pas compliqué. Dans le cas general, l'axiome du choix est requis. On peut d'ailleurs même montrer que l'axiome de choix est équivalent au théorème de Krull.

Correction de l'exercice I.3. :

$\Longrightarrow$: Soit $I \neq \{0\}$ un ideal et $x \in I\backslash\{0\}$. Alors, vu que x est inversible, on a que $xA = A \subset I$.
$\Longleftarrow$: Soit $x \in A$ non nul. Alors $\langle x \rangle = A$ et donc on dispose de $y \in A$ $xy = 1$. Ainsi, A est un corps
Le 2eme point provient direct du fait que $Ideal(A \times B) = Ideal(A) \times Ideal(B)$ en général.

Correction de l'exercice I.9. :

1. Soit $xy \in I$. Supposons que $x, y \notin I$ alors $I + \langle x \rangle = I + \langle y \rangle = A$ par maximalité de I et donc on dispose de $a, b \in A$ $i, j \in I$ $1 = ax + i = by + j$ d'où $1 = abxy + axj + byi + ij \in I$ ce qui est absurde. L'inverse est en général faux. En effet, $\langle X \rangle \subset \mathbb{K}[X, Y]$ est premier mais n'est pas maximal (considérer $\langle X, Y \rangle$)
2. Soit (p) un ideal premier avec $p \geq 0$. $p = 0, p = 1$ conviennent et donc on supposera désormais que $p \geq 2$. Si p est non premier (au sens usuel) alors $p = ab$ avec $a, b \geq 2$ et, dans ce cas, $a, b \notin \langle p \rangle$ mais $ab \in \langle p \rangle$. Ainsi, p est premier est au sens usuel.
   Réciproquement, si $p \geq 2$ est un nombre premier (au sens usuel) alors $\langle p \rangle$ est même maximal (voir plus bas).
3. Soit (p) un ideal maximal avec $p \geq 0$. Il est alors clair que $p \neq 0, 1$ et donc $p \geq 2$. Par les deux questions précédantes on sait alors que p est un nombre premier (au sens usuel). Réciproquement, si $p \geq 2$ est un nombre premier (au sens usuel) alors $\langle p \rangle$ est maximal. En effet, si on prend $x \notin \langle p \rangle$ alors $x \wedge p = 1$ et donc, par l'arithmétique usuelle, on a une relation de Bezout qui oblige que $1 \in \langle p \rangle + \langle x \rangle$ et donc $\langle p \rangle$ est maximal. Remarquer au passage que les ideaux non triviaux premiers concident avec ceux maximaux. Ce n'est pas une coincidence, voir $III.6.$.
4. - Déja fait dans l'exercice précédent
   - $\{0\}$ est premier $\Longleftrightarrow \forall a, b \in A$ $ab = 0 \Longrightarrow a = 0$ ou $b = 0 \Longleftrightarrow A$ est intègre
   - $\{0\}$ est radical $\Longleftrightarrow \forall x \in A$ $\exists n \in \mathbb{N}^* x^n = 0 \Longrightarrow x = 0 \Longleftrightarrow$Le seul nilpotant de A est $0 \Longleftrightarrow A$ est réduit.
5. $\Longrightarrow$: Posons I l'unique ideal maximal de A. Alors A n'intersecte pas $U(A)$ et donc $I \subset J$. Prenons maintenant $x \in J$. x n'étant pas inversible, on a que $\langle x \rangle$ est un idéal strict de A. Par Krull, il est contenu dans un idéal maximal, ici I par unicité et donc $I = J$.
   $\Longleftarrow$: Tout ideal I maximal de A ne doit pas intersecter $U(A)$ et donc $I \subset J$. J étant un idéal strict de A, on obtient par maximalité que $I = J$
6. Par la question précédante, ceci est équivalent à dire que $I = \{x \in A,\ x = 0 \text{ ou } x^{-1} \notin A\}$ est un ideal.
   (a) $0 \in I$
   (b) Soit $x, y \in I$. Alors $x + y \in I$. En effet, $x + y = 0$ est trivial et $x + y \in U(A)$ est impossible car sinon

Correction de l'exercice III.10. :

1. $a^n - 1 = (a - 1)(\sum_0^{n-1} a^k)$ et donc forcément $a = 2$ si $a^n - 1$ est premier.
2. Supposons que $n = mx$ avec $m \geq 3$ impair, alors $a^n + 1 = (a^x)^m - (-1)^m = (a^x + 1)(\sum_0^{m-1} (-1)^{m-1-k} a^{xk})$ ce qui est incompatible avec la primalité de $a^n + 1$.
3. Supposons que cet ensemble est fini et notons le A. Posons $M = (2 \prod_{a \in A} a)^2 - 1$. Il est clair que $M \equiv -1[4]$ et aucun element de A ne divise M. Par conséquent, tous les diviseurs de M (qui sont tous impaires) sont congrus à 1 modulo 4 et donc $M \equiv 1[4]$, ce qui est faux.

* *
*

Document compilé par Issam Tauil le 23/05/2022 pour cpge-paradise.com. Ceci est une version incomplète du cours, elle risque donc de contenir des imprécisions et/ou des erreurs.