Rappels sur les anneaux et les corps.

Préparation à l'Agrégation, ENS de Cachan. Claire RENARD.

Septembre 2012

1 Rappels sur les anneaux.

1.1 Définitions : caractérisations d'anneaux.

A est un anneau commutatif, unitaire, d'unité notée 1.

Définition 1 (Anneau intègre)**.** *L'anneau A est* ***intègre*** *si pour tous a et $b \in A$ tels que $ab = 0$, alors $a = 0$ ou $b = 0$.*

Définition 2 (Anneau noethérien)**.** *Un anneau A est* ***noethérien*** *si, de facon équivalente,*
- *(i) Tout idéal I de A est de type fini.*
- *(ii) Toute suite croissante d'idéaux de A est stationnaire.*
- *(iii) Tout ensemble non vide d'idéaux admet un élément maximal pour l'inclusion.*

Définition 3 (Anneau principal)**.** *Un anneau A est* ***principal*** *s'il est intègre et tout idéal est principal (i.e. de la forme (a), où $a \in A$).*

Définition 4 (Anneau factoriel)**.** *Un anneau A est* ***factoriel*** *si :*
- *(0) A est intègre.*
- *(E) Pour tout $a \in A \setminus \{0\}$, il existe $u \in A^\times$ et $p_1, \dots, p_r$ irréductibles tels que $a = up_1 \dots p_r$.*
- *(U) La décomposition précédente est unique à permutations près et aux inversibles près.*

Définition 5 (Anneau euclidien)**.** *Un anneau A est* ***euclidien*** *si*

1. *A est intègre.*
2. *A est muni d'une* ***division euclidienne****, i.e. il existe une fonction (appelée* ***stathme****) $v : A \setminus \{0\} \to \mathbb{N}$ telle que si a et $b \in A$ avec $b \neq 0$, il existe q et r dans A tels que $a = bq + r$ et ($r = 0$ ou $v(r) < v(b)$).*

Théorème 6 (Hilbert)**.** *Si A est noethérien, alors $A[X]$ est noethérien.*

Théorème 7 (Gauss)**.** *Si A est factoriel, alors $A[X]$ est factoriel.*

Proposition 8. *L'anneau $A[X]$ est principal si, et seulement si, A est un corps.*

$$\begin{tikzcd} & & \text{FACTORIEL} \arrow[r, Rightarrow] \arrow[dd, dash, dotted, "\text{ATTENTION!!!}"] & \text{INTEGRE} \\ \text{EUCLIDIEN} \arrow[r, Rightarrow] & \text{PRINCIPAL} \arrow[ur, Rightarrow] \arrow[dr, Rightarrow] & & \\ & & \text{NOETHERIEN} & \end{tikzcd}$$

ATTENTION : si A est factoriel, il n'est pas nécessairement noethérien. De même, si A est noethérien, il vérifie la propriété (E), mais pas nécessairement (U) et n'est donc pas nécessairement factoriel.

1.2 Exemples.

- $\mathbb{Z}$, $k[X]$ où k est un corps, $\mathbb{Z}[i]$ sont euclidiens.
- $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais pas euclidien.
- $k[X_n, n \in \mathbb{N}]$ est factoriel mais pas noethérien.
- $\mathbb{Z}[i\sqrt{5}]$ est intègre, noethérien, mais pas factoriel.
- Si A est un anneau principal qui n'est pas un corps, alors $A[X]$ est factoriel et noethérien, mais n'est pas principal. L'anneau $\mathbb{R}[X, Y]$ est lui aussi factoriel, noethérien, mais pas principal.

1.3 Idéaux et arithmétique.

Si I est un idéal de A, il y a bijection entre les idéaux $J \supseteq I$ et les idéaux de l'anneau quotient A/I.

Définition 9 (Idéal propre)**.** *Un idéal I de A est dit* ***propre*** *s'il est distinct de A.*

Définition 10 (Idéal premier)**.** *Un idéal I de A est* ***premier*** *s'il est propre et que l'anneau A/I est intègre.*

Autrement dit, I est premier si c'est un idéal propre et pour tous a et $b \in A$, si $ab \in I$, alors $a \in I$ ou $b \in I$.

Définition 11 (Idéal maximal)**.** *Un idéal I est dit* ***maximal*** *si c'est un idéal propre et maximal pour l'inclusion : si J est un idéal de A contenant I, alors $J = I$ ou $J = A$.*

Autrement dit, l'idéal I est maximal si, et seulement si l'anneau quotient A/I est un corps.

$$\text{IDEAL MAXIMAL} \Longrightarrow \text{IDEAL PREMIER}$$

Pour tout $a \in A$, on note (a) l'idéal engendré par a.
Soient a et $b \in A$.

- a **divise** b, noté $a|b$ s'il existe $c \in A$ tel que $b = ac$. De manière équivalente, $a|b \iff (b) \subseteq (a)$.
- a et b sont **premiers entre eux** si pour tout $d \in A$ tel que $d|a$ et $d|b$, alors $d \in A^\times$.
- a et b sont **associés** si $a|b$ et $b|a$, ce qui équivaut à $(a) = (b)$. Si de plus l'anneau A est intègre, cela revient à dire qu'il existe $u \in A^\times$ tel que $a = ub$.

Soit $p \in A$. p est dit **irréductible** si

1. $p \neq 0$ et $p \notin A^\times$
2. si $p = ab$, alors $a \in A^\times$ ou $b \in A^\times$.

Autrement dit, les seuls diviseurs de p sont les éléments inversibles et les associés de p.

$p \in A \setminus \{0\}$ est dit **premier** si (p) l'est.
Lorsque A est intègre, on a :

$$\text{ELEMENT PREMIER} \Longrightarrow \text{ELEMENT IRREDUCTIBLE}$$

Proposition 12. *Soit A un anneau intègre vérifiant la propriété (E) (par exemple noethérien et intègre). Alors les assertions suivantes sont équivalentes :*

1. *A vérifie la propriété (U) (et donc A est factoriel).*
2. ***Lemme d'Euclide :*** *pour tout p irréductible, si $p|ab$, alors $p|a$ ou $p|b$.*
3. *p est irréductible si, et seulement si p est premier.*
4. ***Théorème de Gauss :*** *si $a|bc$ et a est premier avec b, alors $a|c$.*

2 Rappels sur les corps.

Définition 13 (Extension de corps.). *Soit k un corps. Une extension de k est (K, i) où K est un corps et $i : k \to K$ est un morphisme d'anneaux unitaires.*

Remarque 14. *Comme k est un corps, le morphisme i est injectif.*

Le morphisme i est donc souvent sous-entendu, et on considère que k est inclus dans K, noté $(K : k)$ ou $\begin{array}{c} K \\ | \\ k \end{array}$.

Le corps K est naturellement muni d'une structure de k-espace vectoriel (puisque si $\lambda \in k$ et $x \in K$, $\lambda.x = \lambda x \in K$).

Définition 15 (Degré d'une extension.). *Lorsque* $\dim_k(K)$ *est finie, l'extension est dite **finie**. La dimension* $\dim_k(K)$ *est notée* $[K : k]$ *et appelée **degré de l'extension**.*

Théorème 16 (De la base télescopique.). *Le degré d'une extension est multiplicatif. Autrement dit, si $(L : K)$, $(K : k)$ et $(L : k)$ sont trois extensions avec $(L : k)$ finie, alors les deux autres extensions sont aussi finies et $[L : k] = [L : K][K : k]$.*

Si $(K : k)$ est une extension et $\alpha \in K$, on note $k[\alpha] := \{P(\alpha),\ P \in k[X]\}$. C'est le sous-anneau de K engendré par k et α.

ATTENTION : En général, $k[\alpha]$ et $k[X]$ ne sont pas isomorphes, voir la suite !

Si $E \subset K$, on note $k(E)$ le plus petit sous-corps de K contenant k et E.

Définition 17. *L'extension $(K : k)$ est dite **monogène** s'il existe $\alpha \in K$ tel que $K = k(\alpha)$.*

Si $\alpha \in K$, on a $k[\alpha] \subseteq k(\alpha) = \{P(\alpha)/Q(\alpha),\ P, Q \in k[X],\ Q(\alpha) \neq 0\}$.

Soit $\phi : k[X] \to k[\alpha]$ le morphisme d'anneaux défini par $\phi(1) = 1$ et $\phi(X) = \alpha$. Par définition, ϕ est surjectif.

Proposition 18. *Soit $(K : k)$ une extension de corps et $\alpha \in K$. Les propriétés suivantes sont équivalentes.*

- *(i) Le morphisme ϕ n'est pas injectif. Autrement dit, il existe un polynôme $P \in k[X]$ non nul et tel que $P(\alpha) = 0$.*
- *(ii) L'anneau $k[\alpha]$ est un k-espace vectoriel de dimension finie.*
- *(iii) L'anneau $k[\alpha]$ est un corps.*
- *(iv) $k[\alpha] = k(\alpha)$.*

Définition 19. *Si $\alpha \in K$ vérifie une des assertions de la proposition précédente, α est dit **algébrique** sur k. Sinon, il est **transcendant**.*

Lorsque α est transcendant, ϕ est un isomorphisme entre $k[\alpha]$ et $k[X]$.

Définition 20 (Polynôme minimal.). *Si α est algébrique, il existe un unique polynôme unitaire μ_α de $k[X]$ tel que le noyau de ϕ soit engendré par μ_α : $\ker(\phi) = (\mu_\alpha)$. C'est le **polynôme minimal** de α.*

Par définition, $k[\alpha] \simeq k[X]/(\mu_\alpha)$, et $[k[\alpha] : k] = \deg(\mu_\alpha)$.

Remarque 21. *Si $k[\alpha]$ est un corps, alors l'idéal engendré par μ_α est maximal, et donc μ_α est* irréductible *sur $k[X]$.*

Définition 22 (Corps de rupture.). *Soit $P \in k[X]$ **irréductible**. Une extension $(K : k)$ de k est un **corps de rupture** pour P si $K = k(\alpha)$ avec $P(\alpha) = 0$.*

Existence du corps de rupture et unicité à isomorphisme près : $K \simeq k[X]/(P)$.

Définition 23 (Corps de décomposition.). *Soit $P \in k[X]$ non nécessairement irréductible. Une extension $(K : k)$ de k est un **corps de décomposition** pour P si :*

1. *Dans $K[X]$, le polynôme P est un produit de facteurs de degré 1 ("P a toutes ses racines dans K").*
2. *L'extension de corps $(K : k)$ est minimale pour cette propriété.*

Existence du corps de décomposition et unicité à isomorphisme près. On le note $\mathrm{Dec}_k(P)$.

3 Quelques critères d'irréductibilité de polynômes.

Soit A un anneau factoriel et K son corps des fractions.

Définition 24. *Si $P \in A[X]$ est un polynôme, le* **contenu** *de P, noté $c(P)$, est un pgcd des coefficients de P. Autrement dit, si $P = a_nX^n + \ldots + a_1X + a_0$, $c(P) = \mathrm{pgcd}\,(a_n, \ldots, a_0)$ (défini aux inversibles près).*

Si le contenu de P est inversible, P est dit ***primitif****.*

Proposition 25. *Les polynômes de $A[X]$ irréductibles sont :*

1. *Les constantes $p \in A$ irréductibles dans A.*
2. *Les polynômes de degré au moins un primitifs et irréductibles dans $K[X]$.*

D'où : il suffit d'étudier l'irréductibilité des polynômes de $K[X]$, où K est un corps.

Question : Soit $P \in K[X]$. Est-il irréductible ?

3.1 Identification.

On écrit $P = QR$ où Q est R sont deux polynômes de $K[X]$. Montrer que Q ou R est un polynôme constant.

Par exemple, si le degré de P est 2 ou 3, et que P n'a pas de racine dans K, P est irréductible. La condition reste nécessaire mais n'est plus suffisante lorsque $\deg(P) \geq 4$.

3.2 Critère d'Eisenstein.

Proposition 26 (Criètre d'Eisenstein.)**.** *Soit $P = a_nX^n + \ldots + a_1X + a_0 \in A[X]$ primitif. Supposons qu'il existe un élément irréductible $p \in A$ tel que*

1. *p ne divise pas a_n.*
2. *Pour tout $i = 0, \ldots, n-1$, p divise a_i.*
3. *p^2 ne divise pas a_0.*

Alors P est irréductible dans $K[X]$, et donc aussi dans $A[X]$ puisqu'il est primitif.

3.3 Réduction.

Théorème 27. *Soit $P = a_nX^n + \ldots + a_1X + a_0 \in A[X]$ primitif.*

Supposons qu'il existe un idéal premier I de A tel que :

1. *L'image de a_n par la projection canonique $A \to A/I$ est non nulle.*
2. *L'image de P dans $A/I[X]$ est irréductible dans $(A/I)[X]$ ou $Frac(A/I)[X]$.*

Alors P est irréductible dans $K[X]$ et donc dans $A[X]$.

3.4 Utilisation d'extension(s) de corps.

Proposition 28. *Soit d le degré de P. Le polynôme P est irréductible dans $K[X]$ si, et seulement si pour toute extension L de K avec $[L : K] \leq d/2$, P n'a aucun racine dans L.*

Y penser notamment lorsque l'on est dans un corps fini !

Proposition 29. *Soit $P \in k[X]$ un polynôme irréductible de degré n et K une extension de k de degré m premier avec n. Alors P est encore irréductible dans $K[X]$.*

C'est évidemment faux si l'on ne suppose plus n et m premiers entre eux ! ! !

Un dernier critère (auquel on ne pense pas forcément) : montrer que P est le polynôme minimal d'un certain élément α dans une extension du corps K.