A sera un anneau intègre, unitaire, commutatif
$\mathbb{K}$ est un corps.

I - Anneaux factoriels, principaux et euclidiens

a) Idéaux :

Def 1 : Un idéal est dit premier si $\forall a,b \in A$ tel que $ab \in I$ alors $a \in I$ ou $b \in I$.

Def 2 : Un idéal I propre est dit maximal, si quelque soit J un idéal tel que $I \subset J \subset A$ alors $I = J$ ou $J = A$

Prop 3 : Un idéal maximal est premier.

Prop 4 : I est un idéal premier $\Leftrightarrow A/I$ intègre

Prop 5 : I est un idéal maximal $\Leftrightarrow A/I$ est un corps.

App 6 : Construction de corps finis

Def 7 : Un idéal I est dit principal si il existe $a \in A$ tel que $I = aA$.

Def 8 : Deux idéaux I et J sont dit premier entre eux si $I + J = A$.

b) Anneaux factoriels, anneaux principaux :

Def 9 : A est un anneau factoriel si $\forall a \in A$, il existe une famille d'irréductible $(P_i)_{i \in [\![1,n]\!]}$ $2 \in \mathbb{Z}$ distinct, une famille d'entier $(\alpha_i)_{i \in [\![1,n]\!]}$ et $u \in A^\times$ tel que $a = u \times \prod_{i=1}^{n} P_i^{\alpha_i}$ et cette écriture est unique à inversible et permutation des irréductibles près.

Ex 10 : $\mathbb{Z}[X]$ est factoriel

Prop 11 : A factoriel $\Leftrightarrow A[X]$ factoriel

Def 12 : A est un anneau principal si pour tout idéal de A, il est principal.

Ex 13 : $\mathbb{Z}[i]$, anneau des entiers de Gauss est principal.

Prop 14 : A principal $\Rightarrow$ A factoriel

c) Anneaux euclidiens :

Def 15 : On dit que A est euclidien si il existe une application $\nu : A^* \longrightarrow \mathbb{N}$ appelée stathme euclidien tel que pour tout $(a,b) \in A \times A^*$ il existe $(q,r) \in A^2$ tel que $a = bq + r$ et $\nu(r) < \nu(b)$ ou $r = 0$

ex 16 :
- $\mathbb{K}[X]$ muni du stathme du degré
- $\mathbb{Z}[i]$ avec pour stathme $N : \mathbb{Z}[i]^* \longrightarrow \mathbb{N}$, $a+ib \longmapsto a^2+b^2$

sont des anneaux euclidiens.

Prop 17 : A euclidien $\Rightarrow$ A principal

Cex 18 : Il existe des anneaux principaux non euclidien :
- $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$

Prop 19 : A est un corps $\Leftrightarrow A[X]$ euclidien
$\Leftrightarrow A[X]$ principal.

App 20 : $\mathbb{K}[X_1, \dots, X_n]$ principal $\Leftrightarrow n = 1$

Prop 21 : Les éléments de stathme minimal sont inversibles.

II - Arithmétique des anneaux principaux :

a) Définitions :

Def 22 : Soient $a, b \in A$, on dit que a et b sont premier entre eux si pour tout $d \in A$ tel que $d \mid a$ et $d \mid b$ alors d est inversible

Def 23 :
- On appelera lemme d'Euclide la propriété :
  Soit $b, c \in A$, soit $d \in A$ irréductible
  $d \mid bc \Rightarrow d \mid b$ ou $d \mid c$.
- On appelera propriété de Gauss :
  Soit $a, b, c \in A$, a et b premier entre eux, $a \mid bc \Rightarrow a \mid c$.
- on appelera propriété de Bezout :
  Soit $a, b \in A$, a et b premier entre eux $\Rightarrow aA + bA = A$

Def 24 : Soient a et b dans A^*, un PGCD de a et b est un élément $c \in A^*$ tel que $c \mid a$ et $c \mid b$ et si $d \in A^*$ $d \mid a$ et $d \mid b \Rightarrow d \mid c$

Def 25: Soient $a,b \in A^*$, un PPCM de a et b est un élément $c \in A^*$ tel que $a|c$ et $b|c$ et si $d \in A^*$ tel que $a|d$ et $b|d \Rightarrow c|d$.

Rem 26: Il n'existe pas toujours de PGCD ou de PPCM dans $\mathbb{Z}[i\sqrt{5}]$:
- 3 et $2+i\sqrt{5}$ n'ont pas de PPCM
- 9 et $6+3i\sqrt{5}$ n'ont pas de PGCD

b) Propriétés et propositions:

Prop 27: Bezout $\Rightarrow$ Gauß $\Rightarrow$ Euclide.

Prop 28: A factoriel $\Rightarrow$ Gauß
A principal $\Rightarrow$ Bezout
A factoriel + Bezout $\Leftrightarrow$ A principal.

Prop 29: A principal alors pour $a,b \in A^*$ $aA+bA = pgcd(a,b)A$.

App 30: Algorithme d'Euclide, Algorithme d'Euclide étendu dans les anneaux euclidiens.

Rm 31: Soit $a \in A^*$ tel que $a = u p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ sa décomposition en irréductible. Alors: $A/aA \simeq \prod_{i=1}^{n} A/p_i^{\alpha_i}A$ (Théorème chinois).

App 32: Recherche d'inverse dans $\mathbb{Z}/n\mathbb{Z}$

III - Applications:

a) Entiers de Gauß

Prop 33: $\mathbb{Z}[i]$ est euclidien pour le stathme $N: a+ib \to a^2+b^2$

Prop 34: $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

Prop 35: Les irréductibles de $\mathbb{Z}[i]$ sont les p premier tel que $p \equiv 3[4]$ ou les éléments $a+ib$ tel que a^2+b^2 soit premier

Def 36: On définit $\Sigma = \{n \in \mathbb{N} \mid n = a^2+b^2, a,b \in \mathbb{Z}\}$

Prop 37: Σ est stable par multiplication

Rm 38: Théorème des deux carrés de Fermat
Soit $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ alors $n \in \Sigma \Leftrightarrow \forall p_i \equiv 3[4]$, α_i est pair.

b) Algèbre linéaire.

Soit E un $\mathbb{K}$-ev de dimension finie

Prop 39: $\Phi_u : \mathbb{K}[X] \to End_{\mathbb{K}}(E)$, $P \mapsto P(u)$ est un morphisme d'anneaux
on l'appelle morphisme d'évaluation en u
$\Phi_{u,x} : \mathbb{K}[X] \to E$, $P \mapsto P(u)x$ est un morphisme d'anneaux
on l'appelle morphisme d'évaluation de u en x.

Rm 40: $\ker(\Phi_u)$ et $\ker(\Phi_{u,x})$ sont des idéaux de $\mathbb{K}[X]$ principal.
On définit ainsi le polynôme minimal π_u de u (resp. le polynôme minimal $\pi_{u,x}$ de u en x) comme l'élément unitaire engendrant $(\ker(\Phi_u)$ (resp $\ker(\Phi_{u,x}))$

Prop 41: Il existe $x \in E$ tel que $\pi_u = \pi_{u,x}$

Prop 42: (Lemme des Noyaux)
Soit $Q = P_1 \cdots P_n$ tel que (P_i) deux à deux premier entre eux.
alors $\ker(Q(u)) = \bigoplus_{i=1}^{n} \ker(P_i(u))$ entre autre, si Q est annulateur alors $E = \bigoplus_{i=1}^{n} \ker(P_i(u))$.

c) Irréductibilité de Polynôme:

Soit A factoriel.

Def 43: Soit $Q \in A[X]$, on définit $C(Q)$ comme le PGCD des coefficients de Q, c'est son contenu.
Si $C(Q) = 1$ on dit que Q est primitif.

Prop 44: P est un élément irréductible de $A[X]$ si et seulement si P est irréductible dans $\mathrm{Frac}(A)[X]$ et P primitif.

Thm 45: (Critère d'Eisenstein)
Soit $P \in A[X]$, $P = a_n X^n + \dots + a_0$, soit $\pi \in A$ irréductible tel que
1) $\pi \times a_n$
2) $\forall i \in [0, n-1]$ $\pi \mid a_i$
3) $\pi^2 \times a_0$
alors P irréductible dans $\mathrm{Frac}(A)[X]$, et donc dans $A[X]$ si $C(P) = 1$.

Thm 46: (Réduction)
I un idéal premier de A, $B = A/I$
$P \in A[X]$, $P(X) = \sum_{i=0}^{n} a_i X^i$ tel que $\overline{a_n} \neq 0$ dans B
Alors si $\overline{P}$ irréductible sur B ou $\mathrm{Frac}(B)$, on a P irréductible dans $\mathrm{Frac}(A)[X]$.

Algorithme 47: Factorisation en produit d'irréductible
Algorithme de Berlekamp.
Soit $\mathbb{F}_q$ un corps fini, $P \in \mathbb{F}_q[X]$,
l'algorithme de Berlekamp rend soit P si celui-ci est irréductible soit un diviseur non trivial de P.
étapes: ① Si $P' = 0$, il existe Q tel que $P(X) = Q(X^p)$
R le polynôme dont les racines des coefficients de Q
alors $P(X) = (R(X))^p$ rendre R et fin
② Si $\mathrm{PGCD}(P, P') \neq 1$ alors rendre $\mathrm{PGCD}(P, P')$ et fin
③ Sinon: P a ses facteurs irréductibles distincts.
$A = \mathbb{F}_q[X]/(P)$ une $\mathbb{F}_q[X]$-Algèbre de dimension n.
On considère le morphisme de $\mathbb{F}_q$-ev $F - \mathrm{id}$ sur A où F est le morphisme de Frobenius, on calcul sa matrice dans la base $(1, \overline{X} \dots \overline{X^{q-1}})$, soit r la dimension du noyau. Si $r = 1$ on rend P et on s'arrête.
Si $r \geq 2$
On calcul une base $\mathcal{B}$ du noyau, on choisit V un vecteur de cette base tel que V non constant
On décrit alors les pgcds de P et $V - a$ pour a dans $\mathbb{F}_q$ il existe un a tel que ce pgcd soit non trivial, on rend alors ce pgcd et on s'arrête.

Développements:
- Thm des deux carrés de Fermat
- Critère d'Eisenstein.

Bibliographie:
- Cours d'Algèbre ; Perrin
- Algèbre ; Gourdon
- Contre exemple en Mathématiques, Hauchecorne.
- "Berlekamp": Objectif Agrégation, Beck