Rappelons la définition d'un anneau quotient.
Soit A un anneau (commutatif unitaire) et soit $I \subseteq A$ un idéal. On définit une relation $\sim$ sur A par

$$a \sim b \iff a-b \in I$$

La relation $\sim$ est une relation d'équivalence sur A et on définit

$$A/_I := A/_\sim$$

On munit $A/_I$ de deux lois en définissant

$$\bar{a} + \bar{b} = \overline{a+b}$$
$$\bar{a} \cdot \bar{b} = \overline{ab}$$

On peut vérifier que ces lois sont bien définies en utilisant que I est un idéal. A/I est automatiquement un anneau commutatif unitaire c'est l'anneau quotient de A par I. De plus, l'application

$$\pi : A \to A/_I$$
$$a \mapsto \bar{a}$$

est un morphisme d'anneaux, c'est le morphisme quotient. On a

$$\ker(\pi) = I.$$

On pense à l'anneau $A/_I$ comme l'anneau obtenu à partir de A en imposant que tous les éléments de I sont nuls.

<u>Ex</u>: Soit $A = \mathbb{Z}[X]$ et $I = (X^2-2)$

$$A/_I = \mathbb{Z}[X]/_{(X^2-2)}$$

Si on note $x = \overline{X} \in A/_I$, on a

$$x^2 = (\overline{X})^2 = \overline{X^2} = \overline{2} = \bar{1}+\bar{1} = 2 \cdot 1_{A/_I} = 2$$

dans $A/_I$, car $x^2 - 2 \in I$.

Déf. Soit I un idéal dans un anneau A
I est un idéal premier si A/I est intègre
I est un idéal maximal si A/I est un corps

Prop.: Soit $I \subseteq A$ un idéal.
1) I est premier ssi
   a) $I \neq A$, et
   b) si $ab \in I$, alors $a \in I$ ou $b \in I$ quels que soient $a, b \in A$
2) I est maximal ssi
   a) $I \neq A$, et
   b) Pour tout $a \in A \setminus I$ (A privé de I) il existe $b \in A$ tq $ab - 1 \in I$.

Prop. $I \subsetneq A$ est maximal ssi pour tout idéal $J \subseteq A$ avec $I \subseteq J \subseteq A$ alors $J = I$ ou $J = A$. Autrement dit, un idéal maximal est maximal parmi les idéaux différents de A.

On va montrer que tout anneau non nul contient un idéal maximal. Rappelons le lemme de Zorn:

Lemme de Zorn: Soit $(E, \leq)$ un ensemble partiellement ordonné. Si chaque chaîne de E a un majorant dans E, alors E contient un élément maximal.

Prop. Soit A un anneau et $I \subseteq A$ un idéal strictement contenu dans A. Alors, il existe un idéal maximal m de A contenant I.

Démo.: Soit
$$\mathcal{J} = \{ J \subseteq A \mid J \text{ idéal}, J \neq A \}$$
ordonné par l'inclusion. Vérifions que l'hypothèse du lemme de Zorn est satisfaite pour $(\mathcal{J}, \subseteq)$. Soit $C \subseteq \mathcal{J}$ une chaîne i.e. l'ordre $\subseteq$ est total sur C.

Si $C = \emptyset$, $I \in \mathcal{J}$ est un majorant de C. On peut supposer que $C \neq \emptyset$. Considérons

$$K = \bigcup C = \{x \in A \mid \exists J \in C : x \in J\}$$

On montre que $K \in \mathcal{J}$.
Comme tout élément $J \in C$ est un idéal $\neq A$, $\forall J \in C : 1 \notin J$. D'où $1 \notin K$. D'où $K \neq A$. Montrons que K est un idéal de A.

(i) $C \neq \emptyset$, $\exists J \in C$ idéal de A.
$0 \in J$. D'où $0 \in K$.

(ii) supposons que $x, y \in K$.
$\exists J \in C$ tq. $x \in J$, $\exists J' \in C$ tq $y \in J'$.
Comme C est une chaîne, on a $J \subseteq J'$ ou $J' \subseteq J$. Dans le 1^er^ cas $x \in J \subseteq J'$ et $y \in J'$. D'où $x+y \in J'$ et $x+y \in K$. Dans le 2^ème^ cas $x \in J$ et $y \in J' \subseteq J$. D'où $x+y \in J$ et $x+y \in K$. Au final $x+y \in K$.

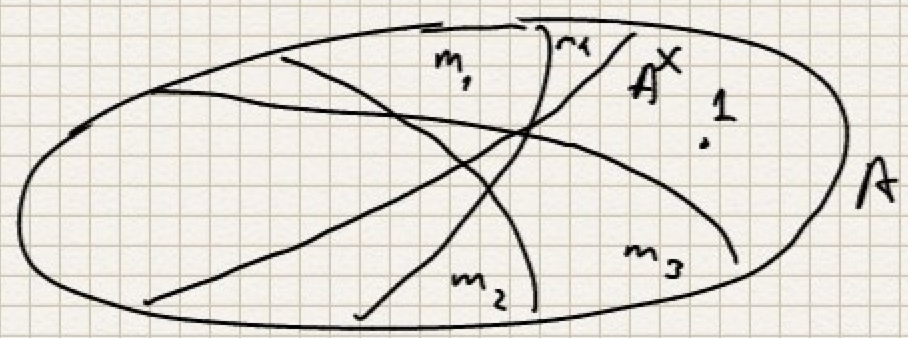
(iii) Si $x \in K$ et $a \in A$, $\exists J \in C$ tq $x \in J$. D'où $ax \in J$ et donc $ax \in K$.

Cela montre que K est un idéal de A strictement contenu dans A, i.e., $K \in \mathcal{J}$.
Par construction, $\forall J \in C : J \subseteq K$, i.e., K est un majorant de C dans $\mathcal{J}$.
L'hypothèse du lemme de Zorn est bien vérifiée. D'où il existe un élément maximal m dans $\mathcal{J}$. D'après la proposition précédente, m est un idéal maximal de A. Il contient I par construction. $\square$

Corollaire Soit $a \in A$ non inversible. Alors il existe un idéal maximal m de A le contenant, i.e., $a \in m$.

<u>Dém.</u> Soit $I = (a) \subseteq A$. Comme a est non inversible, $I \neq A$. Il existe donc un idéal maximal m le contenant. $\square$

Corollaire. Soit A un anneau.
Notons $\mathrm{Max}(A) = \{ m \subseteq A \mid m \text{ idéal maximal} \}$
Alors
$$A = A^\times \cup \Big(\bigcup_{m \in \mathrm{Max}(A)} m \Big)$$
et cette réunion est disjointe i.e.,
$$A^\times \cap \Big(\bigcup_{m \in \mathrm{Max}(A)} m \Big) = \emptyset$$



ou encore
$$A^\times = A \setminus \Big(\bigcup_{m \in \mathrm{Max}(A)} m \Big)$$

Corollaire Tout anneau non nul contient un idéal maximal.
Démo. Appliquer la prop. précédente à l'idéal (0). ∎

On peut le dire encore différemment
tout anneau non nul admet un morphisme surjectif sur un corps.

C'est une façon de passer d'un anneau à un corps. Rappelons une autre construction d'un corps à partir de certains anneaux: le corps des fractions d'un anneau intègre.

Soit A un anneau intègre. Soit $S = A^\times = A \setminus \{0\}$. Définissons une relation $\sim$ sur l'ensemble $A \times S$ par
$$(a, s) \sim (b, t) \iff at = bs \text{ dans } A$$

On peut vérifier que $\sim$ est une relation d'équivalence sur l'ensemble $A \times S$. (On utilise A intègre et $0 \notin S$ pour montrer la transitivité.) On note

$$\mathrm{Frac}(A) = (A \times S)/_{\sim}$$

Ce quotient est aussi noté $S^{-1}A$. La classe d'équivalence du couple (a,s) est notée comme fraction $\frac{a}{s}$ purement formellement :

$$\frac{a}{s} := \overline{(a,s)}$$

On fait de $\mathrm{Frac}(A)$ un anneau en définissant

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

Vérifier que ces lois sont bien définies !
On peut vérifier que $\mathrm{Frac}(A)$ est un anneau commutatif unitaire.
De plus $\frac{a}{s} = 0$ dans $\mathrm{Frac}(A)$ ssi $a = 0$ dans A. Donc $\frac{a}{s}$ est inversible ssi a est non nul et $\left(\frac{a}{s}\right)^{-1} = \frac{s}{a}$ dans ce cas.
Comme $\frac{0}{1} \neq \frac{1}{1}$ dans $\mathrm{Frac}(A)$, $\mathrm{Frac}(A)$ est un corps, dit le <u>corps des fractions</u> de A. De plus, l'application

$$\iota : A \longrightarrow \mathrm{Frac}(A), \quad a \longmapsto \frac{a}{1}$$

est un morphisme d'anneaux injectif.

<u>Ex.</u> 1) Si $A = \mathbb{Z}$, $\mathrm{Frac}(A) = \mathbb{Q}$ et $\iota : \mathbb{Z} \to \mathbb{Q}$ c'est l'inclusion.

2) Si K est un corps et $A = K[X]$, $\mathrm{Frac}(A) = K(X)$ est le corps des fractions rationnelles et $\iota : K[X] \longrightarrow K(X)$ est l'inclusion.

§2 Modules

Déf. Soit A un anneau. Un A-module est un groupe abélien $(M,+)$ muni d'une loi de composition externe

$$A \times M \longrightarrow M$$

notée multiplicativement tel que

1) $(a+b)\cdot m = a\cdot m + b\cdot m$
2) $a\cdot(m+n) = a\cdot m + a\cdot n$
3) $a\cdot(b\cdot m) = (a\cdot b)\cdot m$
4) $1\cdot m = m$

quels que soient $a, b \in A$, $m, n \in M$.

Remarque Un A-module est un A-espace vectoriel lorsque A est un corps.

Soit $(M,+)$ un groupe abélien.
Si $m \in M$ et $a \in \mathbb{Z}$, on écrit

$$am = \begin{cases} \underbrace{m+m+\dots+m}_{a \text{ termes}} & \text{si } a>0 \\ 0 & \text{si } a=0 \\ -(\underbrace{m+m+\dots+m}_{-a \text{ termes}}) & \text{si } a<0 \end{cases}$$

Cela définit donc une loi de composition externe

$$\mathbb{Z} \times M \longrightarrow M,$$

pour tout groupe abélien, et elle vérifie les conditions d'une loi de $\mathbb{Z}$-module. Un groupe abélien est donc automatiquement un $\mathbb{Z}$-module !

Déf Soit M et N des A-modules. Un morphisme de A-modules de M dans N est un morphisme de groupes

$$f : M \longrightarrow N$$

tel que $f(am) = a\cdot f(m)$ $\forall a \in A \, \forall m \in M$.

Remarque si A est un corps et M et N des A-modules, un morphisme de A-modules de M dans N est exactement une application A-linéaire de l'espace vectoriel M dans l'espace vectoriel N.

Remarque. Soient M et N des groupes abéliens. On a $f(am) = af(m)$, pour tout $a \in \mathbb{Z}$ et $m \in M$, si $f : M \to N$ est un morphisme de groupes.
Un morphisme de groupes abéliens est donc automatiquement un morphisme de $\mathbb{Z}$-modules.

Déf. Soit M un A-module. Un sous-A-module de M est un sous-ens. N de M tel que

1) $0 \in N$
2) $x, y \in N \Rightarrow x + y \in N$
3) $a \in A$ et $x \in N \Rightarrow ax \in N$

Remarque Soit A un anneau
on peut considérer A comme A-module en considérant la loi multiplication de A comme loi externe $A \times A \to A$.
A est donc automatiquement un A-module.
plus généralement, d'ailleurs, A^n est un A-module si on définit

$$a \cdot (a_1, \to a_n) = (aa_1, \to aa_n)$$

A considéré comme A-module est donc A^1.
Un sous-A-module de A^1 est la même chose qu'un idéal de A!

Remarque si A est un corps, un sous-A-module est un sous-A-esp vectoriel

Remarque. Si M est un groupe abélien, un sous-groupe de M est automatiquement un sous-$\mathbb{Z}$-module de M.

Prop. Soit $f : M \to N$ un morphisme de A-modules. Alors $\ker(f)$ est un sous-A-module de M et $\operatorname{im}(f)$ un sous-A-module de N.
Démo. exo. $\square$

Prop. Soit M un A-module et $S \subseteq M$ un sous-ensemble. Alors, il existe un plus petit sous-A-module de N de M contenant S. En fait

$$N = \left\{ \sum_{i=1}^{n} a_i s_i \;\middle|\; a_i \in A, s_i \in S, n \in \mathbb{N} \right\}.$$

Démo exo.

Déf. Ce plus petit sous-module est noté (S) et s'appelle le sous-module de M <u>engendré par S</u>. Si $N \subseteq M$ sous-module une <u>famille génératrice</u> de N est un sous-ensemble S de M tq. $(S) = N$

Un sous-ensemble S de M est <u>libre</u> si pour tout sous-ensemble fini $\{s_1, \dots, s_n\} \subseteq S$ on a

$$\sum a_i s_i = 0 \Rightarrow \forall i \; a_i = 0$$

quels que soient $a_i \in A$.

S est une <u>base</u> de M si S est libre et génératrice de M.

Ex Soient

$$e_1 = (1, 0, 0, \dots, 0) \in A^n$$
$$e_2 = (0, 1, 0, \dots, 0) \in A^n$$
$$\vdots$$
$$e_n = (0, 0, \dots, 0, 1) \in A^n$$

Alors $\{e_1, \dots, e_n\}$ est une base du A-module A^n.