Théorie des anneaux, applications à la théorie des nombres

J'essaierai d'écrire aussi le début de l'exposé (sous forme de cours par contre) et de le mettre aussi en ligne sur le site. D'ici là, voici une application en arithmétique de ce que nous avons vu: le résultat final est une description de l'ensemble des sommes de deux carrés dans $\mathbb{N}$. J'ai été moins général que dans l'exposé en termes de théorie des anneaux, je me suis ici plus concentré sur l'arithmétique; je laisse le soin aux élèves les plus intéressés de généraliser au plus ce qui est raconté ici.

1 Fin de l'exposé en exercices

Je mets la fin de l'exposé que j'avais prévu sous forme d'exercices. C'est dans cette fin que se trouvent la plupart des applications en arithmétique que j'avais promises. Je le fais sous forme d'énoncés qui se suivent à peu près, entrelacés de définitions, remarques, etc. Vous pouvez me poser des questions sur les exercices (et autres) par mail si vous voulez.

1. Soit K un corps fini. Montrer que $\prod_{x \in K \setminus \{0\}} x = -1$. En utilisant la forme des idéaux de $\mathbb{Z}$ et la correspondance entre idéaux de A/I et idéaux de A, montrer que pour p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. En déduire que pour p premier, $(p-1)! \equiv -1[p]$. Montrer réciproquement que si $n \geq 2$ vérifie $(n-1)! \equiv -1[n]$, n est premier.
2. En calculant $((\frac{p-1}{2})!)^2$ modulo p, en déduire que si $p \equiv 1[4]$, -1 est un carré modulo p (i.e. il existe a tel que $a^2 \equiv 1[p]$). Montrer réciproquement que si p est un premier impair tel que -1 est un carré modulo p, alors $p \equiv 1[4]$.

Nous venons donc de faire un lien entre les congruences de p modulo 4 et le fait que -1 soit ou non un carré modulo p. On verra en fait que ce dernier point est aussi lié aux possibilités d'écriture de p comme somme de deux carrés.
3. En étudiant les congruences modulo 4 des carrés, montrer que si $n = a^2 + b^2$ (n, a, b des entiers), alors n est congru à $0, 1$ ou 2 modulo 4. En déduire que si p est un premier impair somme de deux carrés, alors $p \equiv 1[4]$.

Nous allons prouver une forme de réciproque et classifier $\{a^2 + b^2, a, b \in \mathbb{N}\}$ à l'aide des décompositions en facteurs premiers.

4. Soit a, b, c des entiers tels que $a = b^2 + c^2$. Soit p un diviseur premier de a tel que $p \equiv 3[4]$. En remarquant que si m n'est pas divisible par p, alors la classe de m est inversible modulo p (Cf. question 1), et en utilisant la réciproque prouvé en en question 2., prouver que p divise b^2 ou c^2.
5. En déduire (si possible sans utiliser la décomposition en facteurs premiers, qu'on a théoriquement pas prouvée dans l'exposé) que p divise b ou c. En déduire que p divise b et c, et donc p^2 divise b^2 et c^2. En déduire que p^2 divise a, et que $\frac{a}{p^2}$ est somme de deux carrés.

6. En déduire que si a est somme de deux carrés, alors pour tout p premier congru à 3 modulo 4, il existe $v \geq 0$ tel que $\frac{a}{p^{2v}}$ soit somme de deux carrés et non divisible par p. (ici on utilise la propriété suivante de $\mathbb{N}$: si P est une propriété des entiers telle qu'il existe n tel que $P(n)$ est vraie, alors il existe un tel n minimal.)

7. En déduire que tout nombre qui est somme de deux carrés s'écrit sous la forme $m^2 n$ où n est somme de deux carrés et tout diviseur premier impair de n est congru à 1 modulo 4. Réciproquement, montrer que si $a = m^2 n$ où n est somme de deux carrés, alors a est somme de deux carrés.

Il ne reste donc plus qu'à étudier les sommes de deux carrés qui n'ont que des diviseurs premiers égaux à 2 ou congrus à 1 modulo 4. Démontrons deux choses qui nous permettront de nous ramener aux nombres premiers :

8. En s'inspirant des nombres complexes et de la relation $|zz'|^2 = |z|^2|z'|^2$ (où $|z|$ est le module de z défini pour $z = a + ib$, a, b réels par $\sqrt{a^2 + b^2}$), montrer que si n, m sont somme de deux carrés, alors nm aussi.

On va ensuite montrer la décomposition en facteurs premiers dans un cadre plus général que $\mathbb{Z}$, ce qui permettra de l'adapter pour des anneaux que nous utiliserons aussi. Pour cela il faut quelques définitions.
Définitions : Soit A un anneau (commutatif). $x \in A$ est dit inversible s'il existe y tel que $xy = 1$.
On dit que a divise b (noté $a \mid b$) s'il existe c tel que $ac = b$.
Un élément non inversible $p \in A$ est dit *premier* si dès lors que $p \mid ab$, $p \mid a$ ou $p \mid b$.
Un élément non inversible $q \in A$ est dit *irréductible* si dès lors que $p = uv$, u ou v est inversible.
Quelques questions pour s'approprier un peu ces notions :

9. (a) Quels sont les éléments inversibles de $\mathbb{Z}$? De $\mathbb{Q}$? Plus généralement, d'un corps ? De $C^0(\mathbb{R}, \mathbb{R})$? De $\mathbb{R}[x]$?
(b) Sans utiliser la décomposition en facteurs premiers, montrer que si $p \in \mathbb{Z}$ est premier au sens usuel, il est premier au sens défini ci-dessus. Montrer de même qu'un nombre qui est premier au sens usuel est irréductible.
(c) Quels sont les éléments premiers d'un corps ? Irréductibles ? Plus généralement, expliciter la relation de divisibilité dans un corps.

Définitions : Un idéal $I \subset A$ est dit premier si pour tous a, b, si $ab \in I$ alors $a \in I$ ou $b \in I$.
Un idéal $I \subset A$ est dit maximal si $I \neq A$ et si pour tout idéal J, si $I \subset J$, alors $J = I$ ou $J = A$.

Un anneau A est dit intègre si pour tous a, b, si $ab = 0$ alors $a = 0$ ou $b = 0$.

A nouveau, quelques questions pour s'approprier un peu ces notions:
10. (a) Montrer que si p est premier, alors $(p) = pA = \{px, x \in A\}$ est un idéal premier, et si (p) est un idéal premier, alors p est premier.
(b) Montrer que si (p) est un idéal maximal, p est irréductible.
(c) Montrer que tout corps est un anneau intègre; montrer que la réciproque est fausse.
(d) Montrer que dans un anneau intègre, si p est premier, alors p est irréductible.
(e) Montrer (en utilisant la correspondance des idéaux) que A/I est un corps si et seulement si I est un idéal maximal. Retrouver alors la preuve que $\mathbb{Z}/p\mathbb{Z}$ est un corps.
(f) En explicitant ce que signifie "A/I est intègre" du point de vue de A, montrer que A/I est intègre si et seulement si I est un idéal premier. En déduire des exemples d'anneaux non intègres.
(g) En déduire que tout idéal maximal est premier.
Définition : Soit $\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\}$ l'ensemble des nombres complexes de parties réelle et imaginaire entière.
11. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$. En particulier, c'est un anneau. On l'appelle souvent "anneau des entiers de Gauss".

Soit $N : \mathbb{Z}[i] \to \mathbb{N}$ définie par $N(z) = |z|^2$. Le rapport entre cet anneau et notre problème est que n est somme de deux carrés si et seulement si il est de la forme $N(z)$ pour un $z \in \mathbb{Z}[i]$.

12. (Question un peu astucieuse) Montrer que si $a, b \in \mathbb{Z}[i]$, avec $b \neq 0$, alors il existe $q, r \in \mathbb{Z}[i]$ tels que $a = bq + r$ et $N(r) < N(b)$.

13. En déduire que tout idéal de $\mathbb{Z}[i]$ est de la forme $(z) = z\mathbb{Z}[i]$ pour un certain $z \in \mathbb{Z}[i]$ (penser à la preuve pour $\mathbb{Z}$).

Définition : Un anneau A est dit principal s'il est intègre et si tout idéal $I \subset A$ est de la forme $(x) = xA$ pour un certain $x \in A$.
Ce qui précède montre que $\mathbb{Z}, \mathbb{Z}[i]$ sont principaux.

On a montré en 10. que dans un anneau intègre, donc en particulier dans un anneau principal, tout élément premier est irréductible.
14. Montrer que dans un anneau principal, si q est irréductible, alors (q) est maximal. En déduire que si q est irréductible, il est premier.

Donc dans un anneau principal, les notions d'élément irréductible et d'élément premier coïncident, comme c'est le cas par exemple dans $\mathbb{Z}$. La preuve que tout anneau principal admet une décomposition en élément premiers est un peu longue et peut-être plus conceptuellement difficile, donc elle sera plus guidée.

15. Dans cette question, A désigne un anneau principal fixé. Quand on dira "idéal" ce sera donc "idéal de A", etc.
(a) Soit (I_n) une suite croissante d'idéaux (i.e. pour tout n, $I_n \subset I_{n+1}$). Montrer que $\bigcup_{n\in\mathbb{N}} I_n = \{x \in A \mid \exists n \in \mathbb{N}, x \in I_n\}$ est un idéal.
(b) En déduire que pour une telle suite, il existe $n \in \mathbb{N}$ tel que $I_n = \bigcup_{k\in\mathbb{N}} I_k$ (on utilise ici que A est principal !). Par croissance, c'est donc le cas pour tous les $m \geq n$: on dit que la suite (I_n) est stationnaire. En particulier, pour $m \geq n, I_m = I_n$.
(c) Montrer que $xA = yA$ si et seulement si il existe u inversible tel que $x = yu$. On dit alors que x et y sont associés.
(d) En procédant par l'absurde, et en construisant une suite croissante d'idéaux non stationnaire, montrer que tout élément de A est divisible par au moins un élément irréductible ($\iff$ premier puisqu'on est dans un anneau principal).
(e) En raisonnant par l'absurde, similairement à (d), montrer que tout élément s'écrit comme un produit fini d'éléments irréductibles et un élément inversible : $up_1...p_n$ où chaque p_i est irréductible et u est inversible.
(f) Montrer que cette décomposition est unique à l'ordre des facteurs près, à inversibles près; c'est-à-dire que si $up_1...p_m = vq_1...q_n$ avec p_i, q_i irréductibles, u, v inversibles, alors $m = n$ et il existe une bijection $f : \{1, ..., m\} \to \{1, ..., n\}$ telle que pour tout i, $q_{f(i)}$ et p_i sont associés (i.e. il existe w_i inversible tel que $q_{f(i)} = w_i p_i$) - pour cette question, on utilise que premier est équivalent à irréductible dans un anneau principal.
(g) En se souvenant des inversibles de $\mathbb{Z}$, retrouver le résultat connu pour $\mathbb{Z}$.

16. Déterminer, en fonction de l'application N, les inversibles de $\mathbb{Z}[i]$. En déduire un théorème de décomposition pour $\mathbb{Z}[i]$.

Remarque : Attention ! Il n'y a a priori aucun rapport entre les premiers de $\mathbb{Z}[i]$ et ceux de $\mathbb{Z}$. C'est d'ailleurs de cette interaction entre ces différentes notions de primalité que va venir notre résultat.

Cette proposition nous permet de nous ramener aux premiers. En effet nous savons (question 8.) que l'ensemble des sommes de deux carrés est stable par produit, et s'écrit $\{m^2 n, m \in \mathbb{N}, n \in \mathbb{N}, n$ est somme de deux carrés et tout diviseur premier de n est 2 ou congru à 1 modulo 4$\}$. Quitte à sortir les termes correspondant à 2 dans la décomposition en facteur premiers (car $2 = 1+1 = 1^2+1^2$ est somme de deux carrés), on obtient que cet ensemble est en fait $\{2^k m^2 n, m, k \in \mathbb{N}, n \in \mathbb{N}, n$ est somme de deux carrés et tout diviseur premier de n est congru à 1 modulo 4$\}$. Pour pouvoir le décrire plus explicitement, il suffit alors d'étudier les premiers congrus à 1 modulo 4 qui sont somme de deux carrés.
17. (a) Soit p un premier dans $\mathbb{Z}$. Montrer que si p est une somme de deux carrés dans $\mathbb{Z}$, alors p n'est pas irréductible dans $\mathbb{Z}[i]$.
(b) Soit p un premier dans $\mathbb{Z}$. Montrer que si p n'est pas irréductible dans $\mathbb{Z}[i]$, alors p est somme de deux carrés dans $\mathbb{Z}$.

Ainsi nous avons fait un lien entre l'irréductibilité dans $\mathbb{Z}[i]$ et le fait d'être une somme de deux carrés. Mais nous avons aussi, par la question 10. ,
18. Soit p un premier dans $\mathbb{Z}$, p est irréductible dans $\mathbb{Z}[i]$ si et seulement si $\mathbb{Z}[i]/(p)$ est intègre. Donc p est somme de deux carrés si et seulement si $\mathbb{Z}[i]/(p)$ n'est pas intègre.

La dernière étape de la preuve consiste donc à décrire $\mathbb{Z}[i]/(p)$ en fonction de p, et plus exactement en fonction de ce que -1 est un carré modulo p ou non. Intuitivement, l'existence d'un lien entre ces propriétés vient du fait que l'équation $x^2+1=0$ a deux solutions dans $\mathbb{Z}[i]$ (i et $-i$), et que si -1 est un carré modulo p (disons $a^2 \equiv -1[p]$), quotienter par (p) rajoute deux solutions à cette équation (a et $-a$): elle a donc 4 solutions, mais est de degré 2, ce qui est impossible pour les anneaux intègres (ce petit schéma de preuve peut être formalisé, mais je ne le donne ici que pour l'intuition).

La fin de la preuve repose sur les polynômes. Nous allons donc devoir les définir sur un anneau quelconque. Il est ici important de faire une distinction entre polynômes et fonctions polynômiales: les polynômes sont un outil formel qui permet entre autres d'étudier les fonctions polynômiales, mais ne s'y réduisent pas.

Définition : Soit A un anneau. On appelle anneau des polynômes sur A l'anneau commutatif consitué des sommes formelles $\sum_{k=0}^{d} a_k X^k$, où les $a_k \in A$, et X est juste un symbole, régi par les règles suivantes: $\sum_{k=0}^{d} a_k X^k = 0$ si et seulement si pour tout $k \in \{0,...,d\}, a_k = 0$; $X^0 = 1$, $X^n X^m = X^{n+m}$, et où l'addition et la multiplication sont régies par les associativités, les commutativités, et la distributivité.

Ce qu'on entend dans la dernière phrase est la chose suivante: par exemple si on veut calculer $(X^2+X+1)(X^3+3)$, on effectue une distribution formelle $X^2(X^3+3)+X(X^3+3)+(X^3+3)$, puis une deuxième sur chaque terme $X^2X^3+X^23+XX^3+X3+X^3+3$, puis on s'autorise à utiliser la commutativité de l'addition et de la multiplication, ainsi que les règles expliquées pour obtenir $X^5+3X^2+X^4+3X+X^3+3$, et finalement on obtient $X^5+X^4+X^3+3X^2+3X+3$. Si cette définition ne vous satisfait pas, vous avez tout à fait raison; elle n'est pas extrêmement rigoureuse. Elle est surtout là pour vous aider à comprendre comment les polynômes marchent: la vraie définition (qui suit) n'est pas extrêmement illuminante.
Définition : Soit A un anneau. On appelle anneau des polynômes sur A, et on note $A[X]$ l'anneau construit comme suit :
Ses éléments sont les suites $(a_n)_n \in A^{\mathbb{N}}$ nulles à partir d'un certain rang (i.e. telles qu'il existe n_0 tel que pour tout $n \geq n_0, a_n = 0$);
Son 1 est la suite $(1,0,0,...)$; son 0 est la suite $(0,0,0,...)$;
Si $(a_n)_n$ et $(b_n)_n$ sont de telles suites, on définit $(a_n)_n + (b_n)_n = (a_n+b_n)_n$ et $(a_n)_n \times (b_n)_n = (\sum_{k=0}^{n} a_k b_{n-k})_n$;
On note X la suite $(0,1,0,0,0,....)$, et on note $\sum_{k=0}^{\infty} a_k X^k$ la suite $(a_n)_n$. Si $a_m = 0$ pour tout $m \geq d+1$, on la note aussi $\sum_{k=0}^{d} a_k X^k$.

19. (a) Vérifier que $+, \times$ sont bien définies (au sens où $(a_n)+(b_n), (a_n) \times (b_n)$ sont bien dans $A[X]$ si (a_n) et (b_n) le sont); et que $(A[X], +, \times, 0, 1)$ est un anneau.
(b) Vérifier que X^n (l'élément X à la puissance n) est bien la suite qui vaut 0 partout sauf en n-ième position, où elle vaut 0.
(c) En déduire que si $P = (a_n)$, avec $a_n = 0$ pour $n \geq d+1$, alors $P = \sum_{k=0}^{d} a_k X^k$, ce qui "justifie" la notation indiquée plus haut.
(d) Montrer que pour tout $x \in A$, l'application $ev_x : A[X] \to A$ définie par $(a_n) \mapsto \sum_{k=0}^{\infty} a_k x^k$ est bien définie (les sommes infinies n'ont pas de sens en général...) et est un morphisme d'anneaux.

Maintenant qu'on a cet outil, je peux enfin dévoiler le plan d'attaque de la fin de la preuve: la première étape de cette fin est de justifier cette suite d'isomorphismes (je note $A \simeq B$ pour "il

existe un isomorphisme $A \to B$")

$$\mathbb{Z}[i]/(p) \simeq (\mathbb{Z}[X]/(X^2+1))/(p) \simeq (\mathbb{Z}[X]/(p))/(X^2+1) \simeq (\mathbb{Z}/p\mathbb{Z}[X])/(X^2+1)$$

. Une fois ceci justifié, il ne restera plus qu'à montrer que l'idéal (X^2+1) est premier dans $\mathbb{Z}/p\mathbb{Z}[X]$ si et seulement si -1 n'est pas un carré modulo p.
Une fois ces deux choses justifiées: on pourra conclure: si p est congru à 1 modulo 4, alors -1 est un carré modulo p, donc l'idéal (X^2+1) n'est pas premier dans $\mathbb{Z}/p\mathbb{Z}[X]$, donc $(\mathbb{Z}/p\mathbb{Z}[X])/(X^2+1)$ n'est pas intègre, donc $\mathbb{Z}[i]/(p)$ (qui lui est isomorphe) n'est pas intègre non plus, donc (p) n'est pas premier dans $\mathbb{Z}[i]$, donc il n'est pas irréductible, donc il est somme de deux carrés dans $\mathbb{Z}$.
Ne vous inquiétez pas si ceci est allé un peu vite pour vous, tout sera repris plus en détail après; simplement il faut voir la puissance de ce qu'on a accompli ici: pour quelqu'un qui est habitué aux anneaux, justifier ces choses là n'est pas compliqué, et grâce à un isomorphisme on peut faire le lien entre être une somme de deux carrés, et le fait que -1 soit un carré modulo soi, grâce à des principes abstraits d'algèbre: cela ne peut que nous motiver à faire de l'algèbre si on veut faire de l'arithmétique.

Définition : Soit $P = \sum_{k=0}^{\infty} a_k X^k \in A[X]$ un poynôme. On appelle degré de P et on note $\deg(P)$ le plus grand entier n tel que $a_n \neq 0$ (il existe bien par définition de $A[X]$- par convention $\deg(0) = -\infty$)

20. (a) Soit A un anneau, $P, Q \in A[X]$. Montrer que $\deg(PQ) \leq \deg(P) + \deg(Q)$.
(b) Montrer que si A est supposé intègre, il s'agit en fait d'une égalité. En déduire un contrexemple à l'égalité dans le cas général.

21. (a) Soit A un anneau, $P \in A[X]$, $B = \sum_{k=0}^{d} b_k X^k \in A[X]$. On suppose que b_d est inversible. Montrer qu'il existe $Q, R \in A[X]$ tels que $P = BQ + R$ avec $\deg(R) < \deg(B)$.
(b) En déduire que si A est un corps, alors tout idéal de $A[X]$ est de la forme $(P) = P \cdot A[X]$ pour un certain P (penser à la preuve pour $\mathbb{Z}, \mathbb{Z}[i]$)

22. Soit $f : \mathbb{R}[X] \to \mathbb{C}$ définie par $f(P) = P(i)$ (la restriction de ev_i à $\mathbb{R}[X]$, avec les notations du 19.(d)), et g la restriction de f à $\mathbb{Z}[X]$.
(a)Montrer que $X^2+1 \in \mathrm{Ker}(f)$, et qu'il n'y a pas de polynôme de degré 1 dans $\mathrm{Ker}(f)$.
(b) En déduire que $\mathrm{Ker}(f) = (X^2+1)\mathbb{R}[X]$.
(c) En déduire que $\mathrm{Ker}(g) = (X^2+1)\mathbb{Z}[X]$.
(d) En déduire que $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$, avec un isomorphisme qui envoie la classe de X modulo X^2+1 sur i, et l'image de $\mathbb{Z}$ modulo X^2+1 sur $\mathbb{Z}$.

23. Soit $f : A \to B$ un isomorphisme d'anneaux, I un idéal de A et J un idéal de B tel que $f(I) = J$. Montrer que A/I est isomorphe à B/J.
24. Soit A un anneau, I, J deux idéaux tels que $I \subset J$. Notons $\pi : A \to A/I$ le morphisme canonique de projection, et J/I l'image de J par π. Montrer que J/I est un idéal de A/I, et que $A/J \simeq (A/I)/(J/I)$.

25. Montrer que $\mathbb{Z}[X]/(p) \simeq \mathbb{Z}/p\mathbb{Z}[X]$.

26. (a) Déduire des exercices 22 et 23 le premier isomorphisme de la suite :

$$\mathbb{Z}[i]/(p) \simeq (\mathbb{Z}[X]/(X^2+1))/(p)$$

.
(b) En considérant les idéaux (p), (X^2+1) et $(p)+(X^2+1)$ de $\mathbb{Z}[X]$, déduire de l'exercice 24 le deuxième isomorphisme de la suite:

$$(\mathbb{Z}[X]/(X^2+1))/(p) \simeq (\mathbb{Z}[X]/(p))/(X^2+1)$$

(c) Déduire le troisième isomorphisme de la suite grâce aux exercices 25 et 23 :

$$(\mathbb{Z}[X]/(p))/(X^2+1) \simeq (\mathbb{Z}/p\mathbb{Z}[X])/(X^2+1)$$

27. Déduire des exercices 26., 21., et 10. que p est premier dans $\mathbb{Z}[i]$ si et seulement si X^2+1 est premier dans $\mathbb{Z}/p\mathbb{Z}[X]$, et donc que p est somme de deux carrés dans $\mathbb{Z}$ si et seulement si X^2+1 n'est pas premier dans $\mathbb{Z}/p\mathbb{Z}[X]$.
28. (a) Grâce à l'exercice 21., remarquer que $P \in A[X]$, pour A un corps, est premier si et seulement s'il est irréductible. En étudiant les degrés, montrer qu'un poynôme de degré 2 dans un corps est irréductible si et seulement s'il n'a pas de racine.
(b) En déduire que X^2+1 est premier dans $\mathbb{Z}/p\mathbb{Z}[X]$ si et seulement si -1 n'est pas un carré modulo p.
(c) Conclure: si p est premier (dans $\mathbb{Z}$) congru à 1 modulo 4, alors p est somme de deux carrés dans $\mathbb{Z}$.

29. Faire une conclusion globale : décrire les entiers qui sont somme de deux carrés d'entiers en fonction de leur décomposition en facteurs premiers.