Groupes et Arithmétique. Notes du cours MI4 2014.

Daniel Bennequin *

Table des matières

*Institut de Mathématiques de Jussieu, Université Paris VII, France

1 Divisibilité et congruences

1.1 Entiers naturels, relations d'équivalence, entiers relatifs

La suite ordonnée des nombres naturels, $1, 2, 3, 4, ...$ est une des plus anciennes découvertes humaines. Il est difficile de dire à quand remontent les opérations d'addition et de multiplication avec des nombres naturels, à quand remonte la description de leurs principales propriétés, comme commutativité, associativité et distributivité. Ces opérations paraissent déjà maîtrisées dans les tablettes sumériennes, ou les papyrus égyptiens. Leur formalisation algébrique apparaît dans les traités arabes ou européens de la fin du Moyen-âge. Entre temps il y avait eu la découverte des sciences mathématiques en Grèce, vers -600 : les démonstrations, les rapports entre nombres et figures géométriques.
Un point important est la compatibilité des opérations algébriques sur les nombres entiers naturels avec l'ordre : si $a \leq a'$ et $b \leq b'$ on a $a + b \leq a' + b'$ et $ab \leq a'b'$, de plus si une des inégalités de départ est stricte les inégalités d'arrivée sont strictes. Bien que le zéro ne soit apparu que plus tard (on le dit venant des Indes), il est pratique pour formuler la plupart des résultats, par exemple la *division euclidienne* de $n \geq 0$ par $m > 0$:

Théorème : il existe un unique entier naturel $q \geq 0$ et un unique entier naturel r, tel que $0 \leq r < m$, et $n = mq + r$.

Démonstration : la suite $0, m, 2m, 3m, ...$ des multiples de m dépasse (ou égale) n pour la première fois à qm, alors $n - qm$ est strictement plus petit que m.
On appelle q le quotient de la division euclidienne de n par m et r son reste.

L'ensemble des nombres entiers naturels se note $\mathbb{N}$, et ceux qui sont différent de 0 forment $\mathbb{N}^*$.

Des bilans de recettes et dépenses sont présents dans les plus anciens documents. Les scribes égyptiens ou sumériens tenaient des comptes, les babyloniens aussi. Les phéniciens, et tous les peuples méditerranéens utilisèrent les mathématiques pour faire du commerce. Sans le dire (comme Monsieur Jourdain pour la prose), ils manipulaient des classes d'équivalence des paires (n, m), pour la relation $(n, m) \sim (n', m')$ si et seulement si $n + m' = n' + m$. En effet, deux tableaux de recette et dépense, n, m et n', m' donnent le même bilan à cette condition.

Nous notons maintenant $n - m$ cette classe, et savons que $n - m = n' - m'$ équivaut bien à cette relation.

Définition : une relation d'équivalence R sur un ensemble E est donnée par un ensemble de paires (x, y) d'éléments de E, qu'on note $x \sim y$, et qui vérifient les trois axiomes suivant :
(i) réflexivité, $\forall x \in E, x \sim x$, (ii) symétrie, $\forall x, y \in E, x \sim y \Rightarrow y \sim x$, (iii) transitivité, $\forall x, y, z \in E, (x \sim y \quad et \quad y \sim z) \Rightarrow x \sim z$.

A une relation d'équivalence R sur E on associe une partition P_R de E : il suffit de mettre ensemble les éléments équivalents. La réflexivité entraîne que la réunion des parties ainsi obtenues est E tout entier, et la transitivité entraîne que les parties sont disjointes.
Inversement pour toute partition P de E il existe une unique relation d'équivalence $R = R_P$ sur E telle que $P = P_R$.
Par définition le quotient E/R est l'ensemble des classes, i.e. une classe dans E fait un élément dans E/R.

Image : pour illustrer la notion de relation d'équivalence et d'ensemble quotient on dessine un patatoïde avec des objets dedans qu'on relient par des chemins lorsqu'on les veut équivalents, puis on entoure les paquets, et on les referme en oubliant ce qui est dedans pour obtenir les éléments du nouvel ensemble quotient.

Exemple principal : l'ensemble $\mathbb{Z}$ des entiers relatifs.
Dans ce cas on dit que $(n, m) \sim (n', m')$ lorsque $n+m' = n'+m$. La réflexivité et la symétrie sont évidentes. Pour la transitivité, on fait appel au résultat suivant :
Lemme : soit a, b, c trois entiers naturels, si $a + c = b + c$ alors $a = b$.
Démonstration : si $a < b$ on a $a + c < b + c$ et si $b < a$ on a $b + c < a + c$.
Les classes des (n, m) sont appelées nombres relatifs, et l'ensemble quotient est noté $\mathbb{Z}$.

Remarque : la même démonstration montre que si $c > 0$, et si $ac = bc$ alors $a = b$.

Extension des opérations algébriques à $\mathbb{Z}$: l'addition est donnée par $(a, b) + (n, m) = (a + n, b + m)$ et la multiplication est donnée par

$$(a, b)(n, m) = (an + bm, am + bn). \tag{1}$$

On vérifie facilement que la classe de la somme et celle du produit ne dépendent

que des classes de (a, b) et de (n, m). Cela permet d'additionner et multiplier les nombres relatifs en conservant les propriétés qu'on avait dans $\mathbb{N}$. Mais on a aussi une soustraction qui inverse l'addition :

$$(a, b) - (n, m) = (a, b) + (m, n) = (a + m, b + n). \tag{2}$$

On écrit $(m, n) = -(n, m)$.

De plus on conserve un ordre dans $\mathbb{Z}$: on dit que $(a, b) \leq (n, m)$ si $a + m \leq b + n$.

Attention : la somme reste compatible avec l'ordre mais pas le produit, car si $a \leq b$ et si $c < 0$ alors $ac \geq bc$. Ceci est une source d'erreurs de calcul jamais tarie.

Pratiquement, on va oublier cette construction de $\mathbb{Z}$ par classe d'équivalence, et choisir les uniques représentants dans les classes où soit n soit m vaut 0. Cela donne $(0, n) = -n$ et $(n, 0) = n$. Alors les sommes et les produits se calculent au cas par cas. par exemple $(-n)(-m) = nm$, $(-n)m = -nm$, etc. Cependant il n'est pas inutile de savoir que $\mathbb{Z}$ est la réponse à ce problème des bilans entre recettes et dépenses, et que les opérations algébriques avec les entiers relatifs se justifient par ce biais.

Extension de la division euclidienne à $\mathbb{Z}$: soit n quelconque et $m \neq 0$, il existe un unique couple de nombres (q, r) tel que $n = qm+r$ et $0 \leq r < |m|$.

Remarque : Un autre exemple de construction par classe d'équivalences donne les fractions, c'est-à-dire les *nombres rationnels* : avec les paires d'entiers (naturels, resp. relatifs) (n, m), avec $m \neq 0$, et $(a, b) \sim (a', b')$ si et seulement si $ab' = a'b$.
On vérifie facilement la réflexivité et la symétrie. La transitivitése démontre en utilisant que $ab"b' = a"bb'$ entraîne $ab" = a"b$ si $b' \neq 0$ (signalé en remarque après le lemme analogue pour l'addition). Partant de $\mathbb{Z}$ on obtient $\mathbb{Q}$, le corps des fractions rationnelles. Partant de $\mathbb{N}$ on obtient $\mathbb{Q}_+$, l'ensemble des nombres rationnels positifs, qui s'ajoutent se multiplient et se divisent mais ne se soustraient pas toujours.
Remarque : si on oublie la condition que le second terme de la paire doit être non-nul, toutes les paires sont équivalentes à $(0, 0)$, or $(1, 2)$, par exemple, n'est pas équivalent à $(2, 1)$ car $1 \neq 4$, donc la relation n'est plus transitive, on n'a plus une relation d'équivalence. Par contre, à démontrer en exercice, si on exclue juste $(0, 0)$, la relation re-devient transitive. Que donne-t-elle ?

Est-ce l'addition, ou/et la multiplication s'étendent à ce nouvel ensemble de classes d'équivalence ?

1.2 Euclide, Gauss et Bezout

Définitions et notations : a divise b se note $a|b$. Le *pgcd* de a et b est noté (a, b), il est toujours positif.
Lorsque $(a, b) = 1$, on dit que a et b sont premiers entre eux. Un nombre entier p est dit premier s'il est différent de 1 et qu'aucun nombre autre que ± 1 et $\pm p$ ne le divise. En général on suppose $p > 1$. Exemples.

Théorème de Bezout (dit Bézout) : l'ensemble des nombres de la forme $ax + by$, où x, y parcourent $\mathbb{Z}$, est l'ensemble des multiples de (a, b).
En particulier, il existe des entiers relatifs u, v tels que $d = ua + vb$.

Lemme clé moderne : un sous-ensemble non-vide M de $\mathbb{Z}$ est stable par soustraction si et seulement si il existe $d \geq 0$ tel que $M = d\mathbb{Z}$.

Démonstration : Si $a \in M$ alors $(a - a) \in M$, donc M contient toujours 0. Donc $a \in M$ entraîne que $-a = 0 - a$ est aussi dans M, et si a et b sont dans M on a $a + b = a - (-b)$ dans M, si bien que M est stable par addition, donc stable par multiplication par tous les entiers positif, puisque multiplier a par $b > 0$ revient à ajouter b fois le nombre a à lui-même. M est donc stable par multiplication par tous les entiers relatifs, puisque multiplier a par $-b$ revient à multiplier $-a$ par b. Si M se réduit à 0, la conclusion du lemme est vraie. Sinon, on considère le plus petit nombre strictement positif d contenu dans M. Soit $n \in M$, la division euclidienne de n par d donne $n - qd = r$, avec $0 \leq r < d$. Mais on a aussi $r \in M$ donc $r = 0$, et n est un multiple de d. C.Q.F.D.

On en déduit le théorème de Bezout : en effet l'ensemble $M(a, b)$ des $ax + by$ est stable par soustraction, donc il existe un nombre $e \geq 0$ tel que $M(a, b) = e\mathbb{Z}$. Il existe u et v tels que $e = au + bv$, or le pgcd $d = (a, b)$ divise a et b, donc d divise e. Mais e divise a et b car ils sont tous deux de la forme $ax + by$, le premier en faisant $x = 1, y = 0$, le second en faisant $x = 0, y = 1$, donc $e \leq d$. Si bien que $e = d$.

Corollaire 1 : tout diviseur de a et b divise (a, b).

Un second corollaire est le lemme de Gauss :

Lemme de Gauss : si $(c, a) = 1$ et $c|ab$ alors $c|b$.

Démonstration : Il existe x, y tels que $1 = ax + cy$, donc $b = abx + cby$. Si $ab = cd$ cela donne $b = c(xd + by)$.

Un cas particulier du lemme de Gauss est le lemme d'Euclide :

Lemme d'Euclide : si p est premier et divise ab alors p divise a ou b.

Du théorème de Bezout on déduit aussi :
Corollaire 2 : quelque soit c, on a $(ac, bc) = (a, b)c$.

Démonstration : car les éléments de la forme $xac + ycb$ sont les multiples de (ac, bc), mais ce sont aussi les éléments de la forme $c(ax + by)$ donc les éléments de $c(a, b)\mathbb{Z}$.

De là on déduit :

Théorème 2 : supposons a, b non-nuls ; le nombre $|ab|/d$ est le plus petit commun multiple strictement positif de a et de b, dit *ppcm*. Et tout multiple commun de a et de b est un multiple du *ppcm* de a et b.

Démonstration : en effet, soit m un multiple commun de a et de b, il existe des entiers a', b' tels que $m = aa'$ et $m = bb'$. D'autre part on a $(a/d, b/d) = 1$, sinon d ne serait pas le plus grand diviseur commun de a et de b, donc le corollaire 3 nous dit que $m = (ma/d, mb/d)$. Or $ma/d = b'ba/d$ et $mb/d = a'ab/d$, donc m est un multiple entier de $|ab|/d$. Mais par ailleurs ab/d est un multiple de a et un multiple de b, d'où le résultat.

Remarque : Bézout (1730-1783) vivait avant Gauss (1777-1855), mais Euclide vivait bien avant eux, vers -300 (noter l'entier relatif).
Alors comment avait il fait ? En fait nous allons voir qu'il avait largement anticipé Gauss et Bézout (lui ou des mathématiciens avant lui dont il reprenait les travaux) :

Dans le septième livre des Eléments, Euclide considère deux nombres entiers naturels n, m supérieurs ou égaux à 1, et toutes les paires d'entiers a, b telles que $a/b = m/n$ (i.e. $an = bm$ comme on a vu), avec $a \leq m$, ou ce qui revient au même $b \leq n$. Il existe un plus petit nombre a dans cette liste, appelons le

m_0. Il existe donc n_0 tel que $m_0/n_0 = m/n$.

Lemme clé d'Euclide : il existe un entier $q \geq 1$ tel que $m = qm_0$ et $n = qn_0$.
Démonstration : Faisons la division euclidienne de m par m_0, soit $m = m_0q+r$ avec $0 \leq r < m_0$, et posons $s = n - n_0q$. Puisque $nm_0 = n_0m$ on a

$$nr = n(m - m_0q) = m(n - n_0q) = ms, \tag{3}$$

donc $0 \leq s$, et $s = 0$ si et seulement si $r = 0$. Mais si $r \neq 0$, on aurait une fraction r/s égale à m/n avec $r < m_0$, ce qui n'est pas possible, donc $r = s = 0$.
Exercice : le même calcul montre que lorsque $a/b = c/d$ on a $a/b = (a + c)/(b + d)$.

De ce lemme on déduit les résultats suivants :

Proposition 1 : dans les mêmes conditions, q est le *pgcd* de m et n.
En effet s'il existait un diviseur commun strictement plus grand, on aurait une fraction égale à m/n avec un numérateur strictement plus petit que m_0.

Proposition 2 : tout diviseur de m et n divise q.
En effet, si $m = m'q'$ et $n = n'q'$, on a $m'/n' = m/n$, et en appliquant le lemme à m', n' on obtient q" tel que $m' = m_Oq$" et $n' = n_0q$" d'où $q'q$" $= q$.

On retrouve aussi le lemme de Gauss. En effet, si c est premier avec a et si il existe e tel que $ab = ce$, on a $c/a = b/e$. Mais il n'existe pas d'entier c_0 plus petit que c tel que $c_0/a_0 = c/a$ (pour un certain a_0), sinon le lemme donnerait un diviseur commun de c et a. Donc, d'après le même lemme, c divise b.

Comment retrouve-t-on le Théorème de Bézout ?

Algorithme d'Euclide, pour calculer le pgcd de a et b :

On fait la division euclidienne du plus grand par le plus petit, disons que $a \leq b$. On a $b = aq+r$, alors $r < a$ et les diviseurs communs de a, r sont aussi ceux de a, b. Si $r = 0$ on a $(a, b) = a$, sinon on recommence : $a = rq_1+r_1$ avec $r_1 < r$, à nouveau les diviseurs de a, r sont ceux de r, r_1, etcetera. Comme la suite r_n est strictement décroissante elle atteint 0 en temps fini, et alors (a, b) est le dernier reste non-nul.

Mais, par récurrence, on voit vite que pour tout n, r_n est de la forme $ax_n + by_n$, donc il existe x, y tel que $(a, b) = ax + by$. Attention, ici les x, y

sont en général négatifs.

Tout multiple de (a, b) est donc de cette forme, et dans l'autre sens, tout nombre de cette forme est divisible par (a, b), d'où Bézout.

Remarque : la chose nouvelle par rapport à Euclide dans l'approche moderne est l'introduction des nombres relatifs, et aussi le Lemme clé, qui s'appuie là-dessus, et qui réclame en plus une notion d'ensemble abstrait.

1.3 Décomposition en nombre premiers

Exemples de nombres premiers : $2, 3, 5, 7, ...$ On constate que $p > 1$ est premier en essayant de le diviser par les nombres avant lui, ou mieux avant $\sqrt{p}$.

L'existence de la décomposition de tout entier en produit de nombres premiers est facile à établir :

Soit n un nombre entier strictement plus grand que 1, s'il n'est pas premier il est divisible par deux nombres > 1, si l'un de ceux-ci n'est pas premier on le divise à nouveau. Le procédé se termine en moins de 2^n étapes. Donc n est le produit d'un ensemble fini de nombres premiers, éventuellement répétés :

$$n = p_1^{\alpha_1}....p_n^{\alpha_n}. \tag{4}$$

Théorème 3 (Euclide) : Il existe une infinité de nombres premiers.

En effet, soit $p_1, ..., p_N$ des nombres premiers, le nombre $1 + p_1.p_2...p_N$, est divisible par un nombre premier p, et celui-ci ne peut pas être dans la liste initiale car il diviserait 1.

Remarque : c'est un problème encore largement ouvert de décrire le comportement de la liste des nombres premiers. Par exemple Y.Zhang et J.Maynard viennent tout juste de démontrer qu'il y a une infinité de paires de nombres premiers distants de moins de 600. La conjecture des nombres premiers jumeaux est que 2 peut remplacer 600 : il y aurait une infinité de nombres premiers qui se suivent de 2. Ex. $5, 7,\ 11, 13,\ 17, 19,\ 41, 43,\ ...$
On sait que "en gros" il y a $n/\log(n)$ nombres premiers parmi les n premiers nombres. C'est le contenu du *Théorème des nombres premiers*, du à B.Riemann, J. Hadamard et Ch. De La Vallée Poussin, fin du XIX-ème siècle. Plus précisément, si π_n désigne le nombre de nombres premiers inférieurs ou égaux à n, la suite $\pi_n(\ln(n)/n)$ tend vers 1 lorsque n tend vers l'infini. Cela

entraîne que l'écart entre deux nombres premiers consécutif devient arbitrairement grand, mais pas trop vite. Si p_n désigne le n-ième nombre premier, son ordre de grandeur est $n\ln(n)$.
De l'avis de beaucoup de mathématiciens, l'hypothèse de Riemann est le problème ouvert le plus profond des Mathématiques aujourd'hui ; elle permettrait de décrire encore plus précisément le comportement de l'écart entre deux nombres premiers consécutifs : il existerait une constante C telle que $p_{n+1} - p_n \leq C\sqrt{p_n}\ln(p_n)$. En fait il y a une fonction spéciale qui approche π_n mieux que $n/\ln(n)$, c'est le *logarithme intégral* :

$$Li(n) = \int_e^n \frac{dt}{\ln(t)}, \tag{5}$$

et la conjecture (ou hypothèse) de Riemann dit qu'il existe une constante C' telle que

$$|\pi_n - Li(n)| \leq C'\sqrt{n}\ln(n). \tag{6}$$

Les calculs d'ordinateurs montrent que l'idée est bonne, mais dans ce cas ils n'ont pas vraiment apporté d'idées nouvelles. Par contre tout récemment un programme de calcul sur ordinateurs (réalisé en partie à l'observatoire de Paris) a permis d'achever la démonstration d'une autre célèbre conjecture sur les nombres premiers, faite par Goldbach en 1740 : tout nombre impair positif est somme d'au plus 3 nombres premiers. Ce résultat vient d'être obtenu par Harold Helfgott (péruvien travaillant à l'ENS Ulm, Paris).
L'autre conjecture de Goldbach reste ouverte, elle dit que tout nombre entier positif pair est somme de deux nombres premiers.

Unicité de la décomposition en nombre premiers, déduite du lemme d'Euclide :

Théorème 4 : si $p_1^{\alpha_1}....p_m^{\alpha_m} = q_1^{\beta_1}....q_n^{\beta_n}$, avec des nombres premiers $p_1, ..., p_m$ (resp. $q_1, ..., q_n$) tous différents et rangés en ordre croissant strictement, alors $n = m$, $p_i = q_i$ quelque soit i et $\alpha_i = \beta_i$ quelque soit i.

Démonstration : si la liste est vide c'est que le produit vaut 1 alors le résultat provient de ce que 1 n'est pas divisible. Sinon, prenons p_m il divise le produit de droite, donc il divise l'un des facteurs, donc il divise l'un des q_j, donc il lui est égal. De même de l'autre côté q_n est égal à l'un des p_i. Ceci ne peut arriver que si $p_m = q_m$, puisque c'est le plus grand des deux côtés. En divisant par p_m élevé à la plus petite des deux puissances α_n, β_n, on voit que $\beta_n = \alpha_n$. On recommence avec p_{n-1}, q_{n-1}, etcetera.

Corollaire : soit $n \in Z$ un nombre entier relatif, alors il existe un ensemble fini unique de nombres premiers $p_1 < ... < p_n$ et un ensemble unique de nombres entiers strictement positifs $\alpha_1, ..., \alpha_n$ tels que $n = \varepsilon p_1^{\alpha_1}....p_n^{\alpha_n}$, où $\varepsilon = \pm 1$.
Définitions : on appelle les p_i les diviseurs premiers de n et le nombre α_i s'appelle multiplicité de p_i dans n, on le note aussi $\alpha(n, p_i)$. Par convention on pose $\alpha(n, p) = 0$ lorsque p est premier mais ne divise pas n.

Théorème 5 : le pgcd (resp. ppcm) de $n = \pm p_1^{\alpha_1}...p_k^{\alpha_k}$ et de $m = \pm p_1^{\beta_1}...p_k^{\beta_k}$ (certains α_i ou β_i pouvant être nuls) est égal à $d = p_1^{\gamma_1}...p_k^{\gamma_k}$, où γ_i est l'inf (resp. le sup) de α_i et β_i.
La démonstration, facile, est laissée en exercice.

1.4 Équations en nombres entiers

Définition : étant donnés des entiers $a_1, a_2, ..., a_k$, on note $d = (a_1, a_2, ..., a_k)$ le plus grand diviseur commun de tous les a_i.
Le lemme clé de la section 2 entraîne le résultat suivant.

Théorème de Bézout généralisé : l'ensemble des nombres de la forme $x_1a_1 + ... + x_ka_k$ où les x_i sont dans $\mathbb{Z}$ coïncide avec l'ensemble des multiples de d.
En particulier on peut écrire $d = u_1a_1 + ... + u_ka_k$, avec des u_i dans $\mathbb{Z}$.

Démonstration : d'après le lemme clé (moderne) l'ensemble en question est l'ensemble des multiples d'un nombre entier positif e, et si $e \neq 0$ (c'est-à-dire si l'un des a_i est différent de zéro, le nombre e divise tous les a_i donc il est inférieur ou égal à d. Mais d divise tous les a_i il divise donc toute combinaison entière des a_i donc il divise e, donc il est inférieur ou égal à e. D'où $d = e$.

Théorème 6 : Soit $a_1, ..., a_n, b$ des entiers relatifs ; pour que l'équation suivante en $x_1, ..., x_n$

$$a_1x_1 + ... + a_nx_n = b, \tag{7}$$

possède au moins une solution en nombres entiers, il faut et il suffit que b divise le pgcd $(a_1, ..., a_n)$.

Démonstration : c'est une traduction du théorème de Bézout généralisé.

Cas particulier $n = 2$: Là on a une solution évidente $x_1 = a_2, x_2 = -a_1$

de l'équation homogène $a_1x_1 + a_2x_2 = 0$. Le résultat suivant décrit toutes les autres solutions et le résultat d'après en déduit l'ensemble de toutes les solutions de l'équation avec second membre $b \neq 0$.

Proposition 3 : Soient a, b des nombres entiers différents de zéro, les solutions de l'équation homogène $ax + by = 0$ sont les paires de la forme $(-kb/d, ka/d)$ où $d = (a, b)$ et où k décrit $\mathbb{Z}$.

Démonstration : d'abord on vérifie facilement que $x = -kb/d, y = ka/d$ est bien une solution. Ensuite si x, y est une solution quelconque non-nulle, le nombre $m = -xa = yb$ est un multiple commun de a et de b il est donc divisible par le ppcm de a et de b, qui est $|ab|/d$, donc il existe k dans $\mathbb{Z}$ tel que $m = kab/d$, ce qui donne $xa = -k(b/d)a$ et $yb = k(a/d)b$ d'où le résultat annoncé.

Proposition 4 : si $d|c$, les solutions de $ax + by = c$ sont de la forme $(uc - bk)/d, (vc + ak)/d)$ où $au + bv = d$ et k parcourt $\mathbb{Z}$. Et si d ne divise pas c il n'y a pas de solution entière.

Démonstration : On a déjà montré la seconde assertion. Pour la première on commence par remarquer que si $d = au+bv$ et $c = c'd$ on a $c = (c'u)a+(c'v)b$, donc $x = uc', y = vc'$ est solution de l'équation avec second membre c. Toutes les autres solutions s'en déduisent en ajoutant une solution de l'équation homogène, ce qui donne le résultat annoncé.

Exemple : $6x+34y = 8$. Le pgcd de $6 = 2.3$ et $34 = 17.2$ est 2 qui divise 8, il y a donc au moins une solution, et donc une infinité de solutions. Pour trouver u, v tels que $2 = 6u+34v$ on peut deviner (genre chiffre et lettres) ou appliquer l'algorithme d'Euclide : $34 = 6.5 + 4$, $6 = 4.1 + 2$, d'où $2 = 6 - (34 - 6.5)$ i.e. $2 = 6.6 - 34$. Si bien que, d'après la proposition 4, l'ensemble des solutions de l'équation proposée est

$$x = (6.8 - 34k)/2 = 24 - 17k, \quad y = ((-1).8 + 6k)/2 = 3k - 4. \qquad (8)$$

1.5 Congruences et résidus

Définition de l'ensemble $\mathbb{Z}/n\mathbb{Z}$, pour $n \in \mathbb{N}$: c'est l'ensemble des classes d'équivalence des entiers relatifs modulo n. On note $a \equiv b[n]$, ou $a \equiv bmod.n$, ou $a \equiv b$ s'il n'y a pas de doute sur l'identité de n, et on lit a congrue à b mod.n, et parfois on note $\bar{a}$ la classe de a.
Si $n = 0$ on retrouve $\mathbb{Z}$. Si $n = 1$ on trouve l'ensemble réduit à un élément

$\{0\}$.
Si $n = 2$, le cas le plus important dans la pratique, on trouve "pair" et "impair", le premier est la classe de 0 (on l'identifie avec) et le second la classe de 1 (on l'identifie avec le nombre 0). On peut ajouter modulo 2, $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, et $1 + 1 = 0$. Le signe $\equiv$ peut être utilisé pour être plus clair : $0 + 0 \equiv 0$, $0 + 1 \equiv 1 + 0 \equiv 1$, $1 + 1 \equiv 0$. La soustraction est toujours définie, par exemple $0 - 1 \equiv 1$. On peut aussi multiplier modulo 2 : $0.0 \equiv 0$, $0.1 \equiv 1.0 \equiv 0$, $1.1 \equiv 1$. Toutes les règles du calcul usuel sont satisfaites.
Si $n = 3$, il y a trois classes, $0, 1, 2$ qui s'ajoutent, par exemple $1 + 2 \equiv 0$, se soustraient, par exemple $1 - 2 \equiv -1 \equiv 2$, et qui se multiplient, par exemple $2.2 \equiv 1$.
Il en va de même modulo n : l'addition, la soustraction et la multiplication sont pareillement définies et satisfont les règles usuelles de commutativité, associativité et distributivité. Cela provient du fait que la classe d'une somme ne dépend que des classes des nombres qu'on ajoute et que la classe d'un produit ne dépend que des classes des nombres qu'on multiplie.

La perte de l'ordre n'empêche pas que $a + c = b + c$ entraîne $a = b$, mais elle fait que de $ac = bc$ on ne peut pas déduire $a = b$ en général. Par exemple il y a des diviseurs de 0 autre que 0 si n n'est pas premier. En effet si $n = n'n"$ avec $n' > 1, n" > 1$, on a $n'n" \equiv 0.n"[n]$ mais n' n'est pas 0 modulo n.
Par contre :

Théorème 7 : Dans $\mathbb{Z}/n\mathbb{Z}$, si $ac \equiv bc$ et si c est premier avec n on a $a \equiv b$.

Démonstration : D'après Bézout il existe $x, y \in \mathbb{Z}$ tels que $xn + yc = 1$, donc $yc \equiv 1[n]$. Mais $ac \equiv bc$ implique $(ac)y \equiv (bc)y$, donc $a(cy) \equiv b(cy)$ d'où $a \equiv b$.

Une autre façon d'énoncer ce résultat :

Proposition 5 : un nombre m admet un inverse modulo n (c'est-à-dire un nombre k tel que $mk \equiv 1[n]$) si et seulement si il est premier avec n.

Démonstration : dire que m est inversible modulo n équivaut à dire qu'il existe k et l dans $\mathbb{Z}$ tels que $mk = 1 + ln$, c'est-à-dire, en changeant k en u et l en $-v$, que $um + vn = 1$, qui signifie bien que m est premier avec n en vertu du théorème de Bezout.

Définition : $\mathbb{Z}/n\mathbb{Z}^\times$ est l'ensemble des éléments inversibles pour la multiplication, c'est-à-dire l'ensemble des classes des éléments premiers avec n.

Attention : ne pas confondre $\mathbb{Z}/n\mathbb{Z}^\times$ avec $\mathbb{Z}/n\mathbb{Z}\backslash\{0\}$, parfois noté $\mathbb{Z}/n\mathbb{Z}^*$, qui désigne l'ensemble des éléments non congrues à 0. Ces deux ensembles ne coïncident (pour $n > 1$) que si n est premier.
Définition : la fonction d'Euler $\varphi(n)$ est le nombre d'éléments dans $\mathbb{Z}/n\mathbb{Z}^\times$.

Montrons comment Euler savait calculer $\varphi(n)$:

Lemme 1 : si $n = p^\alpha$ avec p premier et $\alpha \geq 1$, on a $\varphi(n) = p^{\alpha-1}(p-1)$.

Démonstration : entre 0 et $p^\alpha - 1$ les nombres qui ne sont pas premiers avec p^α sont les multiples de p : 0,p,2p,...,$p^\alpha - p$; entre deux de ces nombres qui se suivent il y a $p-1$ nombres qui sont premiers avec p, cela fait $p^{\alpha-1}(p-1)$.

Lemme 2 : soit n et m deux entiers positifs premiers entre eux, et u, v deux nombres entiers relatifs u, v tels que $un + vm = 1$, alors $c = bun + avm$ est premier avec nm si et seulement si a est premier avec n et b premier avec m.

Démonstration : si un nombre premier p divise a et n il divise évidemment c, de même, si un nombre premier q divise b et m il divise évidemment c, donc si c est premier avec nm les deux nombres a et b sont premiers avec n et m respectivement. De l'autre côté, s'il existe un nombre premier p qui divise c et nm, il divise n ou m, d'après le lemme d'Euclide. Supposons qu'il divise n, alors il divise avm mais il ne divise pas vm, sinon il diviserait 1, donc il divise a, ce qui prouve que a n'est pas premier avec n. De même si p avait divisé m il diviserait b donc b ne serait pas premier avec m. Ceci démontre le lemme.

Lemme 3 : si n et m sont premiers entre eux, on a $\varphi(nm) = \varphi(n)\varphi(m)$.

Démonstration : le lemme 2 établit une bijection de l'ensemble des paires (a, b) où a est une classe modulo n de nombre premier avec n et b une classe de nombre premier avec m sur l'ensemble des classes modulo nm des nombres premiers c avec nm. En effet, changer a (resp. b) en $a + kn$ (resp. $b + km$) ne change pas la classe modulo nm de c. De plus, si a, b donne le même c modulo nm que a', b' alors il existe un entier k tel que $(a-a')vm = -(b-b')un+knm$, donc $(a - a')vm \equiv 0[n]$ or $vm \equiv 1[n]$ donc $a \equiv a'[n]$, et on montre de même que $b \equiv b'[m]$. Ceci démontre que l'application sur Z/nmZ définie par la formule du lemme 2 est injective. Enfin, pour voir qu'elle est surjective, on prend c quelconque, et on écrit que $c = cvm + cun$ (puisque $vm + un = 1$).

Remarque : lorsque nous aurons introduit la notion de groupe, nous pourrons

redire tout ça en terme d'isomorphisme de groupes.

Théorème 8 (Euler) : si $n = p_1^{\alpha_1}...p_m^{\alpha_m}$ est la décomposition de n en nombres premiers, on a

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})...(p_m^{\alpha_m} - p_m^{\alpha_m - 1}), \tag{9}$$

ou encore, ce qui revient au même :

$$\frac{\varphi(n)}{n} = (1 - \frac{1}{p_1})...(1 - \frac{1}{p_m}). \tag{10}$$

Il est remarquable que $\varphi(n)/n$ détecte les différents diviseurs premiers de n, sans leurs multiplicités.

Pour montrer à quel point cette formule d'Euler est riche en information, on en déduit la généralisation du célèbre "petit théorème de Fermat" :

Théorème 9 : quelque soit l'entier a premier avec n on a $a^{\varphi(n)} \equiv 1[n]$.

Démonstration : soit $x_1, x_2, ..., x_{\varphi(n)}$ la liste exhaustive des nombres strictement inférieurs à n qui sont premiers avec n, en les multipliant par a et en prenant le reste modulo n, on obtient une autre liste, qui ne peut être qu'une permutation de celle-ci. Donc en faisant le produit de tous on a

$$x_1...x_{\varphi(n)} = ax_1ax_2...ax_{\varphi(n)} = a^{\varphi(n)}x_1...x_{\varphi(n)}, \tag{11}$$

d'où le résultat annoncé d'après la proposition 5.

Corollaire (Fermat) : quelque soit l'entier a différent de zéro modulo p, pour tout nombre premier p, on a $a^{p-1} \equiv 1[p]$.

Une jolie application arithmétique :

Théorème 10 (Fermat, Euler) : pour qu'un nombre premier impair divise une somme de deux carrés premiers entre eux il faut qu'il soit congrue à 1 modulo 4.
En d'autres termes, les facteurs premiers d'une somme de deux carrés premiers entr eux ne peuvent être que 2 ou des nombres premiers de la forme $4m + 1$.

Démonstration : soit p un nombre premier impair, supposons qu'il existe deux nombres entiers positifs a, b premiers entre eux et un nombre entier c tels que

$pc = a^2 + b^2$. Remarquons que ni a ni b ne peuvent être zéro modulo p, sinon ils le seraient tous les deux et du coup ils ne seraient pas premiers entre eux. Alors dans $\mathbb{Z}/p\mathbb{Z}$ on a $a^2 \equiv -b^2$, et si on élève à la puissance $(p-1)/2$, qui est un entier, le petit théorème de Fermat implique $+1 \equiv (-1)^{(p-1)/2}$, donc $p \equiv 1[4]$, car 1 et -1 ne sont congrues modulo n que si $n = 2$.

On en déduit en particulier qu'un nombre premier congrue à 3 modulo 4 ne peut pas être une somme de deux carrés.

En fait, comme Fermat l'avait énoncé (et sans doute démontré) et comme Euler le démontra un siècle plus tard, la réciproque du théorème 10 est vraie : si $p = 4n + 1$ il existe deux entiers a, b premiers entr eux tels que p divise $a^2 + b^2$. Cela équivaut au fait que -1 est un carré modulo p, et ce n'est pas évident ; nous le démontrerons comme application de la notion de polynôme à coefficients dans le *corps* $\mathbb{Z}/p\mathbb{Z}$. Partant de là Euler démontra que tout nombre premier congrue à 1 modulo 4 est lui même une somme de deux carrés (ce que Fermat avait aussi énoncé et peut-être prouvé). Après l'intervention de Gauss, cette déduction se fait facilement en étudiant la divisibilité dans les entiers imaginaires, de la forme $x + iy$, avec $i^2 = -1$.
Exemples : $5 = 1 + 4$, $13 = 4 + 9$, $17 = 1 + 16$, mais $7 = 4 + 1 + 1 + 1$ ou $11 = 9 + 1 + 1$,..., ne peuvent pas être des sommes de deux carrés.

1.6 Exemples d'équations de congruences

Tout d'abord, des résultats établis sur les équations linéaires en nombres entiers on déduit le résultat suivant :

Théorème 11 : soit a, n deux nombres entiers non-nuls premier entre eux, $n \geq 1$, et c un nombre entier quelconque, alors il existe un entier x, unique modulo n tel que $ax \equiv c[n]$.

En effet, x satisfait à l'équation $ax \equiv c[n]$ si et seulement si il existe un nombre entier y tel que $ax + ny = c$. Nous pouvons appliquer la Proposition 4, en faisant $n = b$ et $d = 1$, cela donne toutes les solutions de cette équation : $x = uc - nk, y = vc + ak$, où $au + nv = 1$ et $k \in \mathbb{Z}$.

La démonstration donne $x \equiv uc[n]$, où u vérifie $au + nv = 1$ pour un certain entier v, c'est-à-dire $au \equiv 1[n]$. Ce qui est la formule habituelle $x \equiv a^{-1}c[n]$, valide car a étant premier avec n est inversible modulo n. Inversement, si l'on sait inverser a modulo n, son inverse est unique et l'on trouve une solution de

la congruence $ax \equiv c[n]$ pour n'importe quel c. Ainsi on découvre un procédé de solution des équations $ax + ny = c$ en nombres entiers, lorsque $(a, n) = 1$. Mais trouver $a^{-1} mod.n$ est un autre forme de l'algorithme d'Euclide.

Exemple : $3x \equiv 8[17]$. L'inverse de 3 est 6 car $3.6 = 18 \equiv 1[17]$ donc $x \equiv 6.8[17] \equiv 14[17] \equiv -3[17]$.

A présent, essayons de résoudre des systèmes particuliers de congruences :

Lemme chinois : si le pgcd d de n_1, n_2 divise c_1 et c_2 alors il existe au moins une solution $x \in \mathbb{Z}$ des deux équations suivantes

$$x \equiv c_1 \quad mod.n_1, \qquad x \equiv c_2 \quad mod.n_2, \tag{12}$$

de plus deux solutions quelconques diffèrent par un multiple du ppcm de n_1 et n_2.

Démonstration : soit u_1, u_2 des entiers relatifs tels que $u_1 n_1 + u_2 n_2 = d$, on écrit $c_i = c_i' d$ et on considère le nombre

$$x = c_2' u_1 n_1 + c_1' u_2 n_2. \tag{13}$$

Si on regarde x modulo n_1, on trouve $c_1' u_2 n_2$ qui est congrue à $c_1' d = c_1$, donc $x \equiv c_1[n_1]$. De même on montre que $x \equiv c_2[n_2]$. Ce qui montre que x est une solution. Mais si y est une autre solution, on voit que $x - y$ est congrue à zéro modulo n_1 et modulo n_2, c'est-à-dire qu'il est divisible par n_1 et par n_2, donc $x - y$ est divisible par le ppcm de n_1 et n_2. C.Q.F.D.

Plus généralement, donnons nous k nombres entiers $n_1, ..., n_k$ plus grand que 2, et une liste de k nombres entiers relatifs $c_1, ..., c_k$; le problème est de trouver un nombre entier x qui soit congrue à c_i modulo n_i pour tout i entre 1 et k.

En procédant par récurrence sur k et en utilisant le lemme chinois on obtient :

Théorème 12 : Si les n_i sont deux à deux premiers entre eux, le système d'équations $x \equiv c_i[n_i]$ possède une solution entière. Cette solution est unique modulo le produit $n_1 n_2 ... n_k$.

Exemple : trouver x tel que $x \equiv 1[2]$, $x \equiv 2[7]$, $x \equiv 3[9]$. Comme $7 - 3.2 = 1$, les deux premières équations donnent $x \equiv 2.(-3).2 + 1.1.7 \equiv -5[14] \equiv 9[14]$. Avec la troisième, en utilisant $14.2 - 3.9 = 1$, on obtient $x \equiv 3.2.14 - 9.3.9[126] \equiv 93[126]$.

2 Groupes. Groupes abéliens finis.

2.1 La notion de groupe. Exemples

Les ensembles où une multiplication est définie de sorte que les équations $AX = B$ soient toujours résolubles en X de façon unique, quelque soit A, B, sont particulièrement pratiques. La notion de *groupe* précise cette situation :

Définition : un *groupe* G est un ensemble avec un élément particulier $e = e_G$, appelé son *unité*, où une loi de composition interne μ est définie, c'est-à-dire que pour chaque paire d'éléments a, b dans G un élément $\mu(a, b)$ de G est donné, de sorte que les axiomes suivants soient vérifiés :

$$(i) \quad \forall a, b, c \in G, \quad \mu(\mu(a, b), c) = \mu(a, \mu(b, c)), \tag{14}$$

$$(ii) \quad \forall a \in G, \quad \mu(a, e) = \mu(e, a) = a, \tag{15}$$

$$(iii) \quad \forall a \in G, \exists a' \in G, \mu(a, a') = \mu(a', a) = e. \tag{16}$$

Pour tout a, l'élément a' est unique, car si a" vérifie $\mu(a, a") = \mu(a", a) = e$, en faisant appel à (ii) et (i) on a

$$a' = \mu(a', e) = \mu(a', \mu(a, a")) = \mu(\mu(a', a), a") = \mu(e, a") = a". \tag{17}$$

On dit que a' est l'*inverse* de a, on pourrait le noter a'_μ.
Remarque : dans un groupe G, un inverse à droite est toujours égal à l'unique inverse. En effet, $\mu(x, a) = e$ entraîne $\mu(\mu(x, a), a') = a'$ donc $a' = \mu(x, \mu(a, a'))$ $= \mu(x, e) = x$.

L'unité e est le seul élément à satisfaire à (ii) ; en effet soit e' satisfaisant la même propriété pour tout a, on a

$$e' = \mu(e', e) = e. \tag{18}$$

On dit que e est l'*élément neutre* de la loi μ.
L'axiome (i) se nomme *associativité* de la loi μ.
Le groupe G est dit *abélien*, ou encore *commutatif*, si

$$\forall a, b \in G, \quad \mu(a, b) = \mu(b, a). \tag{19}$$

Théorème 1 : Dans un groupe, quelque soit a, b l'équation $\mu(x, a) = b$ possède une solution x et une seule. De même l'équation $\mu(a, y) = b$ possède une solution y et une seule, et si le groupe n'est pas abélien il arrive que y soit différent de x.

Démonstration : Pour la première équation on pose $x = \mu(a', b)$ et pour la seconde $y = \mu(b, a')$, où a' est l'inverse de a. On vérifie immédiatement que ce sont bien des solutions. L'unicité s'obtient en composant par a' à gauche ou à droite.

Corollaire : Dans un groupe, quelque soit a, b, c, l'équation $\mu(a, c) = \mu(b, c)$ (resp. $\mu(c, a) = \mu(c, b)$) entraîne $a = b$.
En effet a et b sont deux solutions de $\mu(x, c) = \mu(a, c)$ (resp. $\mu(c, x) = \mu(c, a)$).

De façon générale, en théorie des groupes (où on ne suppose pas que les groupes sont abéliens), la notation multiplicative est préférée à l'usage un peu lourd de symboles comme μ, c'est-à-dire que l'on pose très souvent, sans plus préciser,

$$\mu(a, b) = ab. \tag{20}$$

Cela donne l'écriture habituelle des équations : $ax = b$ ou $ya = b$. On a bien $(ab)c = a(bc)$ donc on peut enlever les parenthèses dans les produits. Mais, en général (sauf dans le cas abélien), on doit tenir compte de l'ordre, car ab peut ne pas être égal à ba.
On note alors a^{-1} l'inverse de a, pour tout $a \in G$.
Évidemment, il peut arriver que sur un même ensemble on considère plusieurs lois de groupe, alors il faut bien revenir à l'utilisation de lettres comme μ, μ', etc.

Exercice : supposons qu'on ait une loi interne sur un ensemble E non-vide, notée multiplicativement pour simplifier, qui soit associative (axiome (i)), qui satisfasse au théorème ci-dessus, i.e. quelque soit a, b il existe x, y uniques tels que $ax = b$ et $ya = b$; alors il existe un unique élément e satisfaisant à (ii) et tout élément a un inverse unique à gauche et à droite (axiome (iii)), en d'autres termes E est un groupe.
Solution : soit $a \in E$, et e la solution de $ae = a$, on a pour tout $y \in E$, $yae = ya$, mais tout $b \in E$ s'écrit $b = ya$, donc $be = b$. De même il existe e' tel que $e'a = a$ et on déduit quelque soit b, $e'b = b$. En particulier on a $e = e'e = e'$ (comme pour l'unicité de e). Conclure !

Exemples :
1) $G = \mathbb{Z}$ avec l'élément neutre 0, et la loi $+$, i.e. $\mu(a, b) = a+b$. La vérification est immédiate, l'inverse dans ce cas est l'opposé : $a' = -a$. C'est un groupe abélien.
Attention : $\mathbb{N}$ avec l'unité 0 et la loi $+$ n'est pas un groupe car aucun élément sauf 0 n'a d'inverse. C'est même la raison d'être de $\mathbb{Z}$.

2) $G = \mathbb{Q}^*$, ensemble des fractions rationnelles non-nulles, avec l'unité 1 et la loi de multiplication $\times$, i.e. $\mu(a,b) = ab$. C'est aussi un groupe abélien. De même $\mathbb{R}^*$, nombres réels sauf 0 et $\mathbb{C}^*$, nombres complexes sauf 0.
Attention : $\mathbb{Q}$ (ou $\mathbb{R}$ ou $\mathbb{C}$) avec l'unité 1 et la loi $\times$ n'est pas un groupe car 0 n'a pas d'inverse.
3) $G = \{+1, -1\}$ avec $e = +1$ et la loi $\times$ (ou $\cdot$), i.e. $\mu(a,b) = ab$. Là chaque élément est son inverse. La *table de la loi* est $+1.+1 = +1, +1.-1 = -1.+1 = -1, -1.-1 = +1$. Encore abélien.
4) Un qui ressemble beaucoup : $G = \mathbb{Z}/2\mathbb{Z}$, avec $e = 0$ et la loi $+$. La *table de la loi* est $0+0 = 0, 0+1 = 1+0 = 1, 1+1 = 0$. Encore abélien.
5) Plus généralement $G = \mathbb{Z}/n\mathbb{Z}$, avec $e = 0$ et la loi $+$ est un groupe abélien.
6) Le groupe multiplicatif $G = (\mathbb{Z}/n\mathbb{Z})^\times$ avec l'unité 1, qui possède $\varphi(n)$ éléments, où φ est la fonction arithmétique d'Euler qu'on vient de voir.
7) Enfin un exemple non-abélien, le plus petit possible, il a 6 éléments, c'est $G = \mathfrak{S}_3$, l'ensemble des *permutations* de 3 lettres, i.e. l'ensemble des bijections de $\{1,2,3\}$ sur lui-même. Ici $e = Id$, la bijection qui envoie 1 sur 1, 2 sur 2 et 3 sur 3. La loi interne μ est la composition des applications : $\mu(a,b) = a \circ b$, i.e. $\mu(a,b)(k) = a(b(k))$. Les six éléments de $\mathfrak{S}_3$ sont l'identité, les deux *cycles* d'ordre 3 ($1 \mapsto 2 \mapsto 3 \mapsto 1$, $1 \mapsto 3 \mapsto 2 \mapsto 1$) et les trois *transpositions* (cycles d'ordre 2). Notations (123), (321), (12), (23), (13). Faire la table de la loi.
8) Géométriquement on peut représenter ce groupe par les symétries d'un triangle équilatéral : il y a l'identité, deux rotations de $2\pi/3$ et trois *réflexions*, ou symétries par rapport à des droites. Faire le dessin. Plus généralement, groupe diédral, symétries d'un polygone régulier à n côtés.
C'est à cause de ces exemples non-abéliens que la notation multiplicative ab est préférée, car elle évoque $a \circ b$.

Rappel : une application $f : X \to X'$ d'un ensemble X sur un ensemble X' est dite *injective* si $f(x) = f(y)$ implique $x = y$, et elle est dite surjective si les $f(x)$ remplissent X', i.e. quelque soit $x' \in X'$ il existe au moins un $x \in X$ tel que $f(x) = x'$. On dit que f est bijective si elle est injective et surjective. Dire que f est bijective revient à dire qu'il existe $f' : X \to X$ telle que $f' \circ f = f \circ f' = Id_X$.
Définition : si X est un ensemble quelconque, l'ensemble des bijections de cet ensemble sur lui-même, avec $e = Id$ et la loi de composition $f \circ g$, forme un groupe, appelé groupe des permutations de X et noté $\mathfrak{S}(X)$.
Les cas les plus importants pour nous sont les groupes de permutations des ensembles finis, par exemple le groupe $G = \mathfrak{S}_n$ des permutations de n lettres $\{1, 2, , ..., n\}$. Ce groupe se nomme *groupe symétrique*. Sauf pour $n = 2$ le

groupe $\mathfrak{S}_n$ est non-abélien.
Pour $n = 2$, on a un cas qui ressemble comme deux gouttes d'eau à celui des exemples 2 et 3 : l'unité est $e = Id$ et l'autre élément est la transposition $\tau = (12)$, i.e. $1 \mapsto 2 \mapsto 1$; la table de multiplication de ce groupe est : $e \circ e = e, e \circ \tau = \tau \circ e = \tau, \tau \circ \tau = e$.

Une autre classe très importante de groupes est fournie par l'algèbre linéaire : le groupe $GL_n(\mathbb{R})$ est l'ensemble des matrices inversibles de taille $n \times n$ à coefficients réels, la loi est le produit des matrices et l'élément neutre est la matrice 1_n. Ce groupe se nomme *groupe linéaire*. Avec des coefficients rationnels, on a $GL_n(\mathbb{Q})$, et avec des coefficients complexes et on a $GL_n(\mathbb{C})$. Mais on peut aussi prendre des coefficients entiers, en exigeant que l'inverse soit également à coefficients entiers, alors on obtient $GL_n(\mathbb{Z})$.
D'ailleurs rien n'interdit de considérer des matrices carrées à coefficients dans $\mathbb{Z}/n\mathbb{Z}$ avec la multiplication des matrices ; l'ensemble des matrices à coefficients dans $\mathbb{Z}/n\mathbb{Z}$ dont le déterminant est un élément inversible de $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire un élément de $\mathbb{Z}/n\mathbb{Z}^\times$, forme un groupe.

Les matrices carrés $n \times n$ de déterminant 1 forment aussi un groupe, noté $SL_n(\mathbb{R})$; on peut là aussi considérer des matrices à coefficients dans $\mathbb{Q}, \mathbb{C}$ ou $\mathbb{Z}$. Ce groupe se nomme *groupe spécial linéaire*.
Dès que $n \geq 2$, ces groupes sont non-abéliens. Par exemple, si $n = 2$, la loi de groupe est définie par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \tag{21}$$

En particulier

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{22}$$

mais

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \tag{23}$$

Remarque : d'après les formules de Cramer, toute matrice $n \times n$ à coefficients dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ dont le déterminant vaut 1 est inversible à coefficients dans $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.
Exercice : si une matrice à coefficients entiers relatifs a un inverse à coefficients entiers son déterminant vaut 1 ou -1.

Remarque : étant donné un groupe G d'unité e et de loi μ on peut lui associer le *groupe opposé* G^{op} qui est le même ensemble, avec la même unité mais avec

la loi "retournée"

$$\mu^{op}(a,b) = \mu(b,a). \tag{24}$$

C'est bien un groupe, car l'associativité de μ^{op} découle immédiatement de celle de μ, de même pour la neutralité de e

$$\mu^{op}(a,e) = \mu(e,a) = a, \quad \mu^{op}(e,a) = \mu(a,e) = a; \tag{25}$$

de même pur l'inverse, car si a' est inverse de a pour μ il l'est des deux côtés, donc a' est inverse de a pour μ^{op}.
Exemple : la multiplication des matrices inversibles écrite à l'envers.
Cette remarque est surtout utile pour déduire des formules générales en renversant l'ordre des facteurs.

2.2 Sous-groupes. Morphismes. Images, noyaux. Produit de groupes

Définition : un sous-ensemble H de G est un *sous-groupe* de G si $e \in H$, si $g, h \in H$ entraîne $gh \in H$ et si $g \in H$ entraîne $g^{-1} \in H$.

Proposition 1 : pour qu'un sous-ensemble H d'un groupe G soit un sous-groupe il faut et il suffit qu'il soit non-vide et que pour chaque paire d'éléments (a, b) de H l'élément ab^{-1} appartienne à H.

Exemples : 1) $\{e\}$ tout seul, G tout entier sont des sous-groupes de G.
2) $\{Id, (12)\}$, ou encore $\{Id, (123), (321)\}$, dans $\mathfrak{S}_3$. Mais pas $\{Id, (12), (23)\}$, ni $\{(123), (12)\}$.
3) Dans $\mathbb{Z}/6\mathbb{Z}$, le sous-ensemble $\{0, 3\}$ ou le sous-ensemble $\{0, 2, 4\}$. Exercice : démontrer que avec $\{0\}$ et $\mathbb{Z}/6\mathbb{Z}$ lui-même, ce sont les seuls sous-groupes.
4) Dans $\mathbb{Z}, +$, le "lemme clé moderne" du premier chapitre établissait que les sous-groupes sont les ensembles $d\mathbb{Z}$.
5) $\mathbb{Z}, +$ est un sous-groupe de $\mathbb{Q}, +$, qui est un sous-groupe de $\mathbb{R}, +$.
6) $\mathbb{Q}, \times$ est un sous-groupe de $\mathbb{R}, \times$.
7) $SL_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$.
8) $GL_n(\mathbb{Z})$ est un sous-groupe de $GL_n(\mathbb{Q})$.

Définition : soient G, G' deux groupes (d'unités e, e' respectivement) notés multiplicativement tous les deux, une application $f : G \to G'$ s'appelle un *morphisme* de groupes (ou homomorphisme de groupes), si $f(e) = e'$ et si quels que soient g, h dans G on a $f(gh) = f(g)f(h)$.

Lemme : si f est un morphisme, pour tout g dans G on a $f(g^{-1}) = (f(g))^{-1}$. En effet, $f(g)f(g^{-1}) = f(gg^{-1}) = e'$.

Soit $f : E \to E'$ une application entre ensembles ; rappelons que l'image, notée $f(A)$, d'une partie A de E est l'ensemble des $x' \in E'$ tels que $x' = f(x)$ pour au moins un $x \in A$, et que l'image inverse, notée $f^{-1}(A')$, d'une partie A' de E' est l'ensemble des x dans E tels que $f(x) \in A'$.

Théorème 2 : soit $f : G \to G'$ un morphisme, l'image $f(H)$ d'un sous-groupe H de G est un sous-groupe de G', et l'image inverse $f^{-1}(H')$ d'un sous-groupe H' de G' est un sous-groupe de G.

Démonstration : (i) l'image de H contient l'unité e' de G' car $e \in H$ et $f(e) = e'$, et si g', h' sont des éléments de $f(H)$ la "différence" $g'h'^{-1}$ est aussi un élément de $f(H)$ car il existe g, h dans H tels que $f(g) = g'$ et $f(h) = h'$ d'où

$$f(gh^{-1}) = f(g)f(h^{-1}) = f(g)f(h)^{-1} = g'h'^{-1}; \tag{26}$$

donc $f(H)$ est un sous-groupe de G'.
(ii) l'image réciproque $f^{-1}(H')$ de H' contient l'unité e de G car $f(e) = e'$ appartient à H', et si g, h sont des éléments de $f^{-1}(H')$ la "différence" gh^{-1} est aussi un élément de $f^{-1}(H')$ car $f(g)$ et $f(h)$ étant dans H' l'élément $f(g)f(h)^{-1}$ est dans H', or, comme on vient de le voir $f(g)f(h)^{-1} = f(gh^{-1})$; si bien que $f^{-1}(H')$ est un sous-groupe de G.

Définition : le noyau d'un morphisme $f : G \to G'$ est l'image réciproque de e', il se note $Ker(f)$ et se lit ker, abréviation de kernel.

Exemples : 1) Les morphismes surjectifs $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z}$ lorsque a divise n, le noyau est $a\mathbb{Z}/n\mathbb{Z}$ et il s'identifie à Z/bZ, où $b = n/a$. On voit que la division des entiers se reflète au niveau des groupes.
2) Le groupe alterné $\mathfrak{A}_n$. Exemples de $\mathfrak{A}_3$ et $\mathfrak{A}_4$. Interprétation géométrique, avec le triangle équilatéral et le tétraèdre régulier.
3) L'application *det* est un morphisme de $GL_n(\mathbb{R})$ dans le groupe multiplicatif $\mathbb{R}^*$, son noyau est $SL_n(\mathbb{R})$.
4) L'application *det* est un morphisme de $GL_n(\mathbb{Z})$ dans le groupe multiplicatif $\{\pm 1\}$, son noyau est $SL_n(\mathbb{Z})$.

Définition : soient G, G' deux groupes, d'identités respectives e, e' et de lois respectives μ, μ' on dit que ces groupes sont *isomorphes* s'il existe un morphisme $\varphi : G \to G'$ qui est une bijection.

Alors l'application inverse φ^{-1} de φ satisfait la même propriété en inversant les rôles de G et de G'.

Exemples : 1) les groupes $\{\pm 1\}, \times$, $\mathbb{Z}/2\mathbb{Z}, +$ et $\mathfrak{S}_2, \circ$ sont isomorphes. 2) Le groupe $\mathfrak{S}_3$ est isomorphe au groupe des isométries du plan euclidien qui respectent un triangle équilatéral, appelées symétries du triangle équilatéral.

Définition des groupes cycliques : soit x un symbole, $C_n(x)$ est l'ensemble à n éléments suivant :

$$C_n = \{e, x = x^1, x^2, ..., x^{n-1}\}, \tag{27}$$

avec la loi $x^i x^j = x^k$ où $k \equiv i + j[n]$. On l'appelle groupe cyclique d'ordre n. Il est utile de pouvoir préciser le générateur x, c'est pourquoi nous notons $C_n(x)$. Si y est un autre symbole, l'application qui à y^k associe x^k est un isomorphisme du groupe $C_n(y)$ sur le groupe $C_n(x)$. Si bien qu'il arrive que l'on note C_n et qu'on parle du groupe cyclique à n éléments.

Ce groupe est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$. Un isomorphisme explicite particulier est donné par $\varphi(1) = 0$, $\varphi(x) = 1$ et plus généralement $\varphi(x^k) = k$; on peut voir φ comme une sorte de logarithme (de base x) car $\varphi(xy) = \varphi(x) + \varphi(y)$.
On définit de même $C_\infty(x)$ comme étant l'ensemble $e = x^0, x = x^1, x^2, ..., x^m, ...$, avec la loi $x^i x^j = x^{i+j}$, et on l'appelle groupe *cyclique infini* (ou infini cyclique). Il est isomorphe à $(\mathbb{Z}, +)$. L'isomorphisme est encore donné par $\varphi(x^k) = k$.

Définition des groupes dièdraux : si x, y ont deux symboles, le groupe dièdral $D_n(x; y)$ est l'ensemble à $2n$ éléments suivant :

$$D_n(x; y) = \{e, x = x^1, x^2, ..., x^{n-1}, y, yx, yx^2, ..., yx^{n-1}\}, \tag{28}$$

avec la loi de multiplication qui se déduit des trois relations suivantes :

$$x^n = e, \quad y^2 = e, \quad yxy = x^{n-1} \tag{29}$$

Exercice : ce groupe (non-abélien pour $n \geq 3$) est isomorphe au groupe de symétries du polygone du plan régulier à n côté. Il contient le groupe $C_n(x)$ comme sous-groupe distingué, et le groupe $C_2(y)$, également comme sous-groupe distingué.

Définition du produit de groupes : Si G_1 et G_2 sont des groupes (notés multiplicativement), d'éléments neutres respectifs e_1, e_2 on définit le *groupe*

produit $G_1 \times G_2$, comme l'ensemble des paires (g_1, g_2) avec l'unité (e_1, e_2) et la loi $(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2')$.
On peut bien entendu itérer la définition et définir $G_1 \times G_2 \times G_3$ etcetera, avec les triplets (g_1, g_2, g_3), puis les n-uplets $(g_1, g_2, ..., g_n)$.

Exemple : $\mathbb{Z} \times \mathbb{Z}$ avec 0 et la loi +. C'est un réseau du plan cartésien $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ (qui lui aussi est un groupe produit).
2) $C_n \times C_m$. Par exemple le "groupe de Klein" $C_2 \times C_2$. Et on continue $C_2 \times ... \times C_2$, qu'on peut représenter aussi par $(Z/2Z) \times ... \times (Z/2Z)$, ensemble de suites de 0 et de 1, avec lequel travaille un ordinateur.
3) $C_n \times C_2$ n'est pas isomorphe à D_n pour $n \geq 3$. L'un est abélien, l'autre pas.

Théorème 3 : si n et m sont premiers entre eux, le produit $C_n \times C_m$ est isomorphe au groupe cyclique C_{nm}.

Démonstration : par hypothèse il existe deux nombres entiers u, v tels que $un + vm = 1$; définissons une application φ du produit $C_n \times C_m$ dans C_{nm}, en posant

$$\varphi(x^i, y^i) = z^k \tag{30}$$

où k est le nombre $iun + jvm$ compté modulo nm. D'après le lemme chinois φ est une bijection. Or $\varphi(x^0, y^0) = z^0$ et φ respecte la multiplication, qui correspond à l'addition des exposants. Donc φ est un isomorphisme de groupes.

2.3 Congruence modulo un sous-groupe. Sous-groupes distingués. Groupes quotients

Définition : soit H un sous-groupe de G on définit la relation d'équivalence à gauche modulo H comme suit :

$$g \sim g' mod_g.H \Longleftrightarrow \exists h \in H, \quad g' = gh. \tag{31}$$

Il y a de même une relation à droite $g \sim g' mod_d.H$.
Les classes à gauche sont les gH et les classes à droite les Hg, pour se rappeler quoi est à gauche quoi est à droite penser à la place de g, pas à celle de H.

Autrement dit g, g' sont congrüs à gauche modulo H si leur "différence" (à gauche) $g'^{-1}g$ appartient à H, et sont congrüs à droite modulo H si leur "différence" (à droite) gg'^{-1} appartient à H.

Proposition 2 : ce sont bien des relations d'équivalence.

Démonstration : nous allons traiter le cas de la congruence à gauche, l'autre cas étant en tout point analogue (on peut aussi appliquer le cas à gauche au groupe opposé G^{op} pour avoir celui à droite).
La relation $\equiv_g$ est réflexive car $e \in H$, et $g = ge$, puisque H est un sous-groupe.
La relation $\equiv_g$ sur G est symétrique, car $g' = gh$ entraîne $g = g'h^{-1}$ et h^{-1} appartient bien à H lorsque $h \in H$, puisque H est un sous-groupe.
Enfin la relation $\equiv_g$ est transitive ; en effet, supposons que $g \sim g' mod_g.H$ et que $g' \sim g" mod_g.H$, alors il existe h, h' dans H tels que $g' = gh$ et $g" = g'h'$, et alors $g" = g(hh')$, or hh' est dans H car H est un sous-groupe.

Remarque : en examinant la preuve ci-dessus on constate que si G est un groupe, un sous-ensemble H de G est un sous-groupe si et seulement si la relation de congruence à gauche (ou idem à droite) est une relation d'équivalence. Cela tient au fait que les solutions x de $g' = gx$ sont uniques dans un groupe.

La classe de e est H (à droite comme à gauche), mais aucune autre classe n'est un sous-groupe, puisqu'elle ne contient pas e.

Lorsque le groupe G est non-abélien, il se peut qu'une classe à gauche ne soit pas une classe à droite. Par exemple, considérons le cas du groupe $G = \mathfrak{S}_3$ et du sous-groupe $H = \{Id, (12)\}$, les classes à gauche sont H, $(13)H = \{(13), (132)\}$ et $(23)H = \{(23), (123)\}$, alors que les classes à droite sont H, $H(13) = \{(13), (123)\}$ et $H(23) = \{(23), (132)\}$.
Mais il peut arriver, même dans le cas non-abélien, que les classes à gauche coïncident avec les classes à droite, par exemple, si $H = \{Id, (123), (132)\}$ dans $G = \mathfrak{S}_3$, dans les deux cas les classes sont H et $(12)H = H(12) = G\backslash H$.

Notation : G/H désigne l'ensemble des classes d'équivalence à gauche modulo H et $H\backslash G$ l'ensemble des classes d'équivalence à droite modulo H. On dit que ce sont les espaces homogènes associés à H.

Exemples : 1) $\mathbb{Z}/n\mathbb{Z}$.
2) Si $a|n$, $(\mathbb{Z}/n\mathbb{Z})/\mathbb{Z}/a\mathbb{Z}$. Comme on l'a vu au paragraphe précédent, cet ensemble est en bijection avec $\mathbb{Z}/b\mathbb{Z}$ où $b = n/a$.

Définition : on appelle *indice* de H dans G le nombre des éléments de G/H (c'est le même que le nombre des éléments de $H\backslash G$. On écrit $[G : H]$ pour désigner cet indice.

Attention : en général G/H (ou $H\backslash G$) n'est pas un groupe.

Théorème 4 : Le produit dans G induit un produit dans G/H (resp. $H\backslash G$) si et seulement si l'ensemble G/H coïncide avec l'ensemble $H\backslash G$, i.e. quelque soit g dans G on a $gH = Hg$, ce qui revient à dire que quelque soit g dans G on a $gHg^{-1} = H$.
Dans ce cas, quelque soient g, g' on a $gH.g'H = gg'H$ (et pas seulement l'inclusion $gH.g'H \subset gg'H$). De plus avec la loi induite G/H (resp. $H\backslash G$) est un groupe, appelé groupe quotient de G par H.

Démonstration : a) supposons que la loi interne de G respecte la relation d'équivalence (congruence) à gauche ; cela signifie que quelque soit g, g' on a $gH.g'H \subset gg'H$, ou encore que la classe d'un produit gg' est indépendante du choix de g, g' dans leurs classes, i.e. quelque soit h, h' il existe k tel que $ghg'h' = gg'k$; alors en faisant $g' = g^{-1}$ on trouve que $gHg^{-1}H \subset H$ d'où $gHg^{-1} \subset H$; et l'inclusion dans l'autre sens vient de $g^{-1}Hg \subset H$. a') Le cas des classes à droite se traite de la même façon. b) Réciproquement, si la relation $gHg^{-1} = H$ est satisfaite pour tout g dans G, on a $gH = Hg$, donc $gH.g'H = g(Hg').H = gg'H.H = gg'H$. c) L'unité de G/H est la classe H de e ; le fait que H soit élément neutre est évident, et l'associativité vient de celle de G.

Définition : lorsque la condition $\forall g \in G, gHg^{-1} = H$ est vérifiée par G et H on dit que H est *distingué* (ou *normal*) dans G. Cela se note souvent de la façon suivante : $H \lhd G$.
Attention, un sous-groupe H peut ne pas être distingué dans G tout en étant distingué dans un sous-groupe H' de G qui contient H, par exemple H est toujours distingué dans H lui-même.
Comme les classes à gauche coïncident avec les classes à droite quand H est distingué dans G, la loi de groupe sur G/H ne dépend pas du fait qu'on regarde la relation de congruence à gauche ou à droite.

Exemples : 1) lorsque G est abélien tous ses sous-groupes sont distingués. 2) Si G/H a deux éléments, c'est-à-dire si l'indice $[G : H]$ vaut 2, alors H est distingué dans G. En effet les deux classes ne peuvent être que H et son complémentaire $G\backslash H$. Exemple $\mathfrak{A}_n$ dans $\mathfrak{S}_n$, $SL_n(\mathbb{Z})$ dans $GL_n(\mathbb{Z})$. 3) Cas de $\mathfrak{S}_3$. 4) $SL_n(K)$ dans $GL_n(K)$.

Attention : même si H est distingué dans G, même si G est abélien, il n'est pas possible (en général) de trouver des éléments $g_i, i \in I$ de G, avec un et

un seul élément par classe à gauche modulo H, qui forment un sous-groupe de G. En d'autres termes il peut ne pas exister de morphisme $G/H \to G$ qui inverse la projection $G \to G/H$. Un exemple très simple de ce phénomène est donné par $G = C_4(x)$ et $H = C_2(y)$ engendré dans G par $y = x^2$, en effet les deux classes à gauche modulo H dans G sont $\{e, y\}$ et $\{x, xy\}$; il y a donc quatre possibilités pour relever G/H dans G, i.e. quatre sous-ensembles de G possédant un et un seul élément dans chacune des classes ; ce sont $\{e, x\}$, $\{e, xy\}$, $\{y, x\}$ et $\{y, xy\}$. Les deux derniers ne contiennent pas l'élément neutre, ils ne peuvent pas être des groupes ; le premier n'est pas un groupe puisque $xx = y$ n'y est pas, le second non-plus, puisque $xyxy = xx = y$ n'y est pas. Il faut retenir de cela que la notion de quotient n'est pas la notion de sous-groupe.

2.4 Ordre des éléments d'un groupe.

Définitions : *L'ordre d'un groupe fini* est le nombre de ses éléments. *L'ordre d'un élément* a dans un groupe G est le plus petit $n > 0$ tel que l'on ait $\mu^n(a) = e$ où la suite $\mu^n(a)$ est définie par récurrence : $\mu^0(a) = e$, $\mu^n(a) = \mu(a, \mu^{n-1}(a))$. Lorsque n n'existe pas on dit que l'ordre de a est infini et on écrit $n = \infty$.

Théorème 5 : soit $a \in G$, s'il existe $m \in \mathbb{Z}, m \neq 0$ tel que $a^m = e$, alors l'ordre n de a est fini et il divise m.

Démonstration : l'ensemble M des nombres entiers relatifs k tels que $a^k = e$ forme un sous-groupe de $\mathbb{Z}$; avec notre hypothèse ce groupe ne se réduit pas à 0. On peut donc faire appel au lemme clé du début, ce lemme dit qu'il existe un entier $n > 0$ tel que $M = n\mathbb{Z}$. D'où le théorème.

Théorème 6 : soit G un groupe, et a un élément de ce groupe ; il existe un sous-groupe H de G qui est contenu dans tous les sous-groupes de G contenant a ; ce sous-groupe est unique ; il est isomorphe à C_n où n est l'ordre de a dans G. En fait H est l'ensemble des puissances de a : $H = \{e, a, a^2, ...\}$ et l'isomoprhisme φ de C_n sur H est donné par $\varphi(x) = a$.

La démonstration se fait en partant de la fin de l'énoncé : on note n l'ordre de a et on définit une application de C_n dans G par $\varphi(x^i) = a^i$. C'est un morphisme de groupes, son image $\varphi(C_n)$ est donc un sous-groupe H de G, qui est isomorphe à C_n d'après le théorème 5. De plus il est évident que tout sous-groupe H' de G qui contient a contient H.

Théorème 7 : Si G est fini, l'ordre de H divise l'ordre de G.

Démonstration : chaque classe à gauche (ou à droite) a le même nombre d'éléments, et la classe de e est H.

Corollaire (Lagrange) : si G est fini, l'ordre de tout élément a de G est fini, et divise l'ordre de G.

Comme corollaire, on retrouve le théorème d'Euler et le petit théorème de Fermat.

Théorème 8 : Soit a un nombre entier entre 1 et $n-1$; dans le groupe additif $\mathbb{Z}/n\mathbb{Z}$, l'ordre de a est n/d où $d = (a, n)$ est le pgcd de a et de n.

Démonstration : L'ensemble M des entiers m tels que $ma \equiv 0 mod.n$ forme un sous-groupe de $\mathbb{Z}$, il est donc de la forme $m\mathbb{Z}$ pour un nombre entier positif m. Par définition, l'ordre de a est égal à m. On a $m \neq 0$ car $a \neq 0$. Comme le nombre entier n/d est dans M, il existe un nombre entier strictement positif k tel que $n/d = km$, c'est-à-dire $n = kmd$. D'autre part il existe un nombre entier strictement positif l tel que $ma = ln$, donc $ma = lkmd$, d'où $a/d = lk$. On voit que k divise a/d et n/d, donc $k = 1$ et $m = n/d$. C.Q.F.D.

Corollaire : un élément de $(\mathbb{Z}/n\mathbb{Z}, +)$ est d'ordre n si et seulement si il est premier avec n.
Un tel élément a est donc un *générateur* de $(\mathbb{Z}/n\mathbb{Z}, +)$: l'application φ de $(C_n, \times)$ dans $(\mathbb{Z}/n\mathbb{Z}, +)$ qui envoie 1 sur 0, x sur a et plus généralement x^k sur ka est un isomorphisme de groupe. C'est encore une sorte de logarithme puisque $\varphi(xy) = \varphi(x) + \varphi(y)$ pour tous les éléments x, y de C_n. Son inverse est une sorte d'exponentielle : $\psi(ka) = x^k$.

Exemples : 1) Dans $\mathbb{Z}/6\mathbb{Z}$, seules la classe de 1 et celle de $5 \equiv -1$ sont génératrices. La classe de 2, comme celle de $4 \equiv -2$, est d'ordre 3 et celle de 3 est d'ordre 2, c'est la seule. 2) Dans $\mathbb{Z}/12\mathbb{Z}$, les générateurs sont $1, 5, 7, 11$, les éléments d'ordre 6 sont 2 et 10, ceux d'ordre 4 sont 3 et 9, ceux d'ordre 3 sont 4 et 8, et un seul est d'ordre 2, c'est 6.
3) Dans $\mathfrak{S}_3$, les transpositions sont d'ordre 2, les cycles (123) et (132) sont d'ordre 3. 4) Dans $\mathfrak{S}_4$, l'ordre de (12)(34) est 2, bien que (12)(34) ne soit pas un cycle. 5) Plus généralement, dans $\mathfrak{S}_n$, pour $n \in \mathbb{N}$, $n \geq 1$, l'ordre d'un cycle $(i_1 i_2 ... i_k)$ est égal à k, et l'ordre d'un produit de cycles disjoints est le ppcm des ordres de ces cycles.

Proposition 3 : soit G, G' deux groupes et a et a' des éléments de G et G' respectivement, l'ordre de (a, a') dans le groupe produit $G \times G'$ est le ppcm de ceux de a et a' lorsque ces ordres sont des nombres finis et il est infini si l'ordre de a ou celui de a' est infini.

Démonstration : commençons par le cas où l'ordre de a est un nombre fini n et celui de a' un nombre fini n' ; soit m le plus petit nombre entier strictement positif tel que $(a, a')^m = (e, e')$, on a $a^m = e$ et $a'^m = e'$ donc m est un multiple commun de n et n', mais le ppcm N de n, n' satisfait aussi à $(a, a')^N = (e, e')$ donc $m = N$. Enfin, si a ou a' est d'ordre infini il ne peut exister de nombre entier $m > 0$ tel que $(a, a')^m = (e, e')$, donc (a, a') est d'ordre infini.

2.5 Classification des groupes abéliens finis

Le théorème 3 (équivalent au lemme chinois) entraîne (par récurrence sur le nombre des facteurs) le résultat suivant :

Théorème 9 : si $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$ est la décomposition de n en facteurs premiers, avec $p_1 < p_2 < ... < p_m$, alors il existe un isomorphisme de groupes

$$C_n \to C_{p_1^{\alpha_1}} \times C_{p_1^{\alpha_2}} \times ... \times C_{p_1^{\alpha_m}}. \tag{32}$$

De même on a un isomorphisme entre les groupes additifs (isomorphes aux précédents)

$$\mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_1^{\alpha_2}\mathbb{Z}) \times ... \times (\mathbb{Z}/p_1^{\alpha_m}\mathbb{Z}). \tag{33}$$

Définition : soit α un nombre entier strictement positif ; on appelle *partition* π de α une suite finie décroissante de nombres entiers strictement positifs $\alpha_1 \geq \alpha_2 \geq ... \geq \alpha_m$, tels que $\alpha_1 + \alpha_2 + ... + \alpha_m = \alpha$.
On voit qu'on doit avoir $\alpha \geq \alpha_1$ et $m \leq \alpha$. On appelle m la *longueur* de π et on la note $e(\pi)$.
On note $p(\alpha)$ le nombre de partitions différentes de α.
Lorsque $\alpha = 0$, on a encore une partition $0 = 0$, on convient donc de poser $p(0) = 1$.

Exemple : pour $\alpha = 5$, on a $1+1+1+1+1+1 = 5$, ou $2+1+1+1 = 5$, ou $3+1+1 = 5$, ou $4+1 = 5$, ou $5 = 5$, ou encore $3+2 = 5$ et c'est tout. Ce qui fait 6 partitions différentes, donc $p(5) = 6$. Exercice : calculer $p(n)$ pour $n \leq 6$.

Construction : à tout nombre premier p, tout entier strictement positif α, et toute partition $\pi = \{\alpha_1, \alpha_2, ..., \alpha_m\}$ de α, on associe le groupe suivant

$$C(p; \alpha; \pi) = C_{p^{\alpha_1}} \times C_{p^{\alpha_2}} \times \times C_{p^{\alpha_m}}. \tag{34}$$

c'est un groupe fini d'ordre $p\alpha$.

D'après le théorème 10 seule la partition $\pi = \{\alpha\}$ donne un groupe cyclique.

Lemme 1 : soit $\gamma \leq \beta$ deux nombres entiers positifs ; dans $C_{p^\beta}(x)$, le nombre des éléments d'ordre p^γ est égal à $\varphi(p^\gamma)$, c'est-à-dire $p^{\gamma-1}(p-1)$ d'après le th.8 du chapitre 1.

Démonstration : d'après le théorème 8 l'élément $y = x^a$ dans $C_{p^\beta}(x)$ est d'ordre p^γ si et seulement si le pgcd de a et p^β est égal à $p^{\beta-\gamma}$, ce qui veut dire que $a = qp^{\beta-\gamma}$ avec $1 \leq q \leq p^\gamma - 1$ premier avec p^γ (c'est-à-dire premier avec p), ce qui est la définition de $\varphi(p^\gamma)$.

En particulier, dans $C_{p^\beta}(x)$, il y a un seul élément d'ordre 1 (bien sur), $p-1$ éléments d'ordre p, p^2-p éléments d'ordre p^2, etcetera ; ce qui, à la fin, épuise les p^β éléments de $C_{p^\beta}(x)$.
Le résultat suivant découle immédiatement du lemme 1 :

Lemme 2 : soit $\gamma \leq \beta$ deux nombres entiers positifs ; dans $C_{p^\beta}(x)$, le nombre des éléments d'ordre inférieur ou égal à p^γ est égal à p^γ.

Proposition 4 : soit $\gamma \leq \alpha$ deux nombres entiers positifs, soit $\pi = (\alpha_1, ..., \alpha_m)$ une partition de α (rangée en ordre décroissant) de longueur m, et soit $k = e(\pi; \gamma)$ le nombre des α_i supérieur ou égaux à γ ; alors dans le groupe $C(p; \alpha; \pi)$ le nombre des éléments d'ordre inférieur ou égal à p^γ est égal à $p^{\gamma.k+\alpha_{k+1}+...+\alpha_m}$.

Démonstration : dans le groupe $C(p; \alpha; \pi)$, un élément y de G se représente par un e-uplet $(y_1, ..., y_m)$ où y_i appartient au groupe cyclique $C_{p^{\alpha_i}}(x_i)$, et $y^{p^\gamma} = e$ équivaut à $\forall i, y_i^{p^\gamma} = e_i$ (où e_i désigne l'unité de $C_{p^{\beta_i}}(x_i)$). Pour $i \leq k$ le lemme 2 s'applique, et pour $i > k$ tous les éléments satisfont à l'équation, d'où le nombre de cas distincts annoncés.

Lemme 3 : deux partitions de α qui sont différentes ne peuvent pas donner la même suite $f(\gamma; \pi) = \gamma.k + \alpha_{k+1} + ... + \alpha_m$.

Démonstration : Soit π, π' deux partitions de α. Comme on a $f(1;\pi) = m$, si π et π' n'ont pas la même longueur m elles n'ont pas la même fonction $f(\gamma)$. Supposons donc que π et π' ont la même longueur m, mais qu'elles sont différentes, et considérons le plus grand indice $m-j$ (avec $j \geq 1$) pour lequel π et π' diffèrent ; on a $\alpha_{m-j+1}+...+\alpha_m = \alpha'_{m-j+1}+...+\alpha'_m$, mais $\alpha_{m-j} \neq \alpha'_{m-j}$. Supposons que $\alpha_{m-j} > \alpha'_{m-j}$, il existe alors γ, compris entre α_{m-j+1} et α_{m-j}, tel que $e(\gamma;\pi) = m-j$ et $e(\gamma;\pi') < m-j$, d'où $f(\gamma;\pi) > f(\gamma;\pi')$.

On en déduit le résultat suivant :

Proposition 5 : le groupe $C(p;\alpha;\pi)$ est isomorphe au groupe $C(p';\alpha';\pi')$ si et seulement si $p = p', \alpha = \alpha'$ et $\pi = \pi'$.

A présent démontrons le théorème de classification des groupes abéliens finis. (Bien qu'elle ne soit pas très dure, la preuve n'est pas au programme de l'examen.)

Théorème 11 : tout groupe fini commutatif G est isomorphe à un produit de groupes de la forme $C(p;\alpha;\pi)$. Plus précisément, soit n l'ordre de G, et $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha^k}$ sa factorisation en nombres premiers distincts (avec $p_1 < p_2 < ... < p_k$) ; alors il existe des partitions $\pi_1 = \{\alpha_{1,1}, ..., \alpha_{1,m_1}\}, \pi_2 = ..., \pi_k = ...$ des entiers $\alpha_1, \alpha_2, ..., \alpha_k$ telles qu'il existe un isomorphisme

$$G \to C(p_1;\alpha_1;\pi_1) \times C(p_2;\alpha_2;\pi_2) \times ... \times C(p_k;\alpha_k;\pi_k). \tag{35}$$

De plus les triplets $(p_i;\alpha_i;\pi_i)$ intervenant dans cette factorisation sont uniques ; ce sont les invariants de G à isomorphisme près.

On dit qu'un groupe cyclique $C(p^\beta)$ qui apparaît dans la factorisation de G est un facteur cyclique *primaire* de G, ou facteur *indécomposable* de G. Attention, les nombres p^β sont des invariants de G, mais en général les sous-groupes qu'ils définissent dans G ne sont pas uniquement définis.

Démonstration : la preuve se fait par récurrence sur le nombre n :

posons $p = p_k$ et considèrons le plus grand entier α tel qu'il existe un élément x d'ordre $q = p^\alpha$ dans G ; le plus petit sous-groupe de G contenant x est le groupe cyclique $H = C_q(x)$. Notons $\varphi : G \to G/H$ la projection. Le groupe G/H est d'ordre $n' < n$, on peut donc lui appliquer l'hypothèse de récurrence et le décomposer en facteurs comme dans l'énoncé du théorème, à partir de la décomposition $n' = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha^k-\alpha}$. Choisissons alors des générateurs $x'_i; i \in I$ de tous les facteurs cycliques primaires dans la

décomposition choisie de G/H, et des éléments x_i dans G tels que $\varphi(x_i) = x'_i$.

Supposons x'_i d'ordre N premier avec p, l'ordre de x_i est un multiple de N mais pas forcément N. Cependant l'élément $y_i = x_i^N$ de G appartient au noyau de φ, qui est H, donc il existe un entier n_i tel que $y_i = x^{n_i}$; puisque N est premier avec p^α il existe un entier a tel que $aN + n_i$ soit multiple de p^α (Bézout), donc l'élément $X_i = x_i x^a$ de G est tel que $\varphi(X_i) = x'_i$ et $X_i^N = e$. Par conséquent nous pouvons supposer que les x_i relevant les générateurs x'_i d'ordres premiers avec p ont le même ordre que les x'_i.

Examinons maintenant les x'_i dont l'ordre q' est une puissance p^β de p. L'élément $y_i = x_i^{q'}$ de G est dans H, il s'écrit donc x^{n_i} ; si $n_i = n'_i p^{\gamma_i}$ avec $(n'_i, p) = 1$, l'ordre de y_i est égal à $p^{\alpha-\gamma_i}$, donc l'ordre de x_i est $p^{\beta+\alpha-\gamma_i}$. Comme p^α est maximal, on doit avoir $\gamma_i \geq \beta$, ce qui implique que p^β divise n_i. Écrivons $n_i = m_i q'$ et posons $X_i = x_i x^{-m_i}$; on a $\varphi(X_i) = x'_i$ et $X_i^{q'} = x_i^{q'} x^{-q'm_i} = x^{n_i - n_i} = e$. Si bien que nous pouvons également supposer que les x_i relevant les générateurs x'_i d'ordres puissances de p ont le même ordre que les x'_i.

Dans ce cas, il existe un unique morphisme ψ de G/H dans G envoyant chaque $(x'_i)^k$ sur $(x_i)^k$; ce morphisme satisfait à $\varphi \circ \psi = Id$; son image est un sous-groupe H' de G isomorphe à G/H. Soit ι et ι' les injections respectives de H et H' dans G ; l'application produit $\iota \times \iota'$ du produit $H \times H'$ dans G est un isomorphisme. Ce qui établit le théorème.

Ce théorème est un raffinement de la loi de décomposition des nombres des nombres entiers en facteurs premiers. D'ailleurs on retrouve exactement cette loi en décomposant $\mathbb{Z}/n\mathbb{Z}$.
Les α_i sont les multiplicités des p_i dans n, mais les partitions π_i sont une richesse (et une complexité) nouvelle.
La relation "m divise n" dans les entiers s'étend aux groupes abéliens (ou non-abéliens d'ailleurs) avec la relation H est un sous-groupe de G" (puisqu'alors le cardinal de H divise celui de G).
Mais attention $H \subset G$ n'implique pas qu'il existe un groupe H' tel que G soit isomorphe au produit $H \times H'$! Un exemple très simple de ce phénomène est donné par $G = C_4(x)$ et $H = C_2(y)$ engendré dans G par $y = x^2$, en effet nous avons déjà vu que C_4 n'est pas isomorphe à $C_2 \times C_2$, à la proposition 4.

Remarque : cependant il existe une classe de groupes abéliens, stable par inclusion et par produit, pour laquelle il est vrai que $H \subset G$ entraîne l'existence de $H' \subset G$ avec $G \approx H \times H'$ et $H' \approx G/H$. C'est la classe des groupes abéliens finis sans ramification :
Par définition un groupe abélien fini est dit *totalement non-ramifié* si toutes

les partitions qui interviennent dans sa décomposition sont de la forme $1 + 1 + ... + 1 = \alpha$. Dans ce cas $e(p) = \alpha(p)$ pour tous les nombres premiers p.

Définition : soit π la partition de α associée au nombre premier p pour un groupe abélien fini G ; le nombre m des α_i non-nuls est noté $e(p)$ et s'appelle le *rang* de G en p (ou nombre de générateurs primaires associés à p) ; nous appellerons *ramification* de G en p le nombre $\alpha - e$.

Corollaire 1 du théorème 11 : un groupe abélien fini d'ordre n est cyclique si et seulement si son rang en chaque nombre premier qui divise n est égal à 1.

Démonstration : cela résulte immédiatement du lemme chinois (théorème 3).

Corollaire 2 du théorème 11 : les groupes cycliques d'ordre une puissance d'un nombre premier sont les groupes abéliens finis qui ne peuvent pas s'écrire comme produit de deux groupes à plus de un éléments.
On dit pour ça qu'ils sont *indécomposables*.

Corollaire 3 du théorème 11 : soit p un nombre premier et α un nombre entier naturel, et soit G un groupe abélien fini d'ordre p^α ;
(i) G est isomorphe à $C_p \times ... \times C_p$ (c'est-à-dire G totalement non-ramifié) si et seulement si l'équation $x^p = e$ est satisfaite par tous les éléments de G,
(ii) G est cyclique si et seulement si l'équation $x^p = e$ possède exactement p solutions.

Démonstration : En tenant compte du théorème 11, cela résulte de la proposition 4. En effet, si e désigne le rang de G en p, le nombre de solutions distinctes de l'équation $x^p = e$ dans G est égal à p^e.

Corollaire 4 du théorème 11 : un groupe abélien fini G d'ordre n est cyclique si et seulement si pour chaque diviseur premier p de n l'équation $x^p = e$ possède exactement p solutions.

2.6 Application aux résidus des puissances premières

Définition : on note $R(n)$ le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ des éléments inversibles modulo n, muni de l'unité 1 et de la loi de multiplication induite par celle de $\mathbb{Z}/n\mathbb{Z}$.
Les éléments de $R(n)$ s'identifient donc aux nombres entiers compris entre 1 et $n-1$ qui sont premiers avec n. L'ordre de $R(n)$ est le nombre $\varphi(n)$, qui a

été calculé.
La lettre R est pour résidu, on appellera $R(n)$ le groupe des résidus inversibles modulo n.

Le résultat suivant est une motivation pour passer à l'étude des anneaux, des corps et des polynômes :

Assertion en avance : dans $\mathbb{Z}/p\mathbb{Z}$, quelque soit l'entier m, il n'y a pas plus de m solutions distinctes de $x^m - 1 = 0$.
C'est un cas particulier d'un résultat général sur les équations polynômiales dans les *corps commutatifs*. En effet nous verrons que dans un corps commutatif le nombre des racines d'un polynôme $P(X)$ en une variable de degré m (i.e. les solutions de $P(x) = 0$) est inférieur à m, et nous verrons aussi que $\mathbb{Z}/p\mathbb{Z}$ muni de l'addition et de la multiplication est un exemple de corps commutatif, noté $\mathbb{F}_p$.

Pour le moment, en admettant cette assertion, nous déduisons le résultat suivant sur les résidus inversibles modulo un nombre premier :

Théorème 12 : si p est un nombre premier $R(p)$ est cyclique.

Démonstration : pour p' premier divisant $p-1$, qui est l'ordre du groupe multiplicatif $R(p)$, il y n'y a pas plus de p' solutions de l'équation $x^{p'} = 1$. Mais on sait aussi qu'il y en a toujours au moins p' d'après le corollaire 2 ci-dessus, donc il y en a exactement p'. Alors on applique le corollaire 3 du théorème 11.

Remarque : il est vrai aussi que $R(p^\alpha)$ est cyclique, sauf si $p = 2$ et $\alpha \geq 3$ au quel cas $R(2^\alpha)$ est de rang 2, avec un générateur d'ordre 2 et un d'ordre $2^{\alpha-1}$.

Définition : soit $n, q \in \mathbb{N}$, on dit que $a \in R(n)$ est un *résidu de puissance* q-ième lorsqu'il existe $x \in \mathbb{Z}/n\mathbb{Z}$ satisfaisant à $x^q \equiv a \quad mod.n$.
Lorsque $q = 2$ on parle de résidu quadratique, lorsque $q = 3$ de résidu cubique, etc.

Corollaire 1 du théorème 12 : soit p un nombre premier impair et $a \in R(p)$
L'application $\lambda : a \mapsto a^{p-1/2}$ est un morphisme surjectif de $R(p)$ dans $\{\pm 1\}$.

En effet λ est évidemment un morphisme de groupes multiplicatifs. D'autre part le petit théorème de Fermat dit qu'un élément y de l'image de λ satisfait à $y^2 = 1$, mais il n'y a que deux solutions de cette équation dans $R(p)$ d'après le théorème 12, qui sont $+1$ et -1.

Enfin, puisque $R(p)$ est cyclique d'ordre $p-1$, il existe un générateur z d'ordre $p-1$; si $a = z^{2m'}$, en posant $a' = z^{m'}$ on a $a^{p-1/2} = a'^{p-1} \equiv 1$ d'après le petit théorème de Fermat, donc $\lambda(a) = 1$, mais du coup, si $a = zz^{2m'}$ on a $a^{p-1/2} \equiv z^{p-1/2}$ qui est congru à -1 sinon z ne serait pas générateur.

Définition : le nombre $a^{p-1/2}$, qui vaut $+1$ ou -1 d'après le résultat précédent, se nomme *symbole de Legendre* de a mod. p et se note $(\frac{a}{p})$.

Corollaire 2 du théorème 12 : $a \in R(p)$ est résidu quadratique modulo p si et seulement si

$$(\frac{a}{p}) = a^{p-1/2} \equiv 1 \quad mod.p \tag{36}$$

Démonstration : puisque $R(p)$ est cyclique, il existe un générateur z d'ordre $p-1$; écrivons $a = z^m$ et $x =^n$, si $x^2 = a$ dans $R(p)$ il existe un entier relatif k tel que $m = 2n + k(p-1)$, c'est-à-dire $m = 2(n + k(p-1)/2$, donc m est pair ; posons $m = 2m'$, il vient

$$a^{p-1/2} = z^{m.(p-1/2)} = z^{m'.(p-1)} = (z^{m'})^{p-1} = 1, \tag{37}$$

en vertu du petit théorème de Fermat.
Inversement supposons que $a^{p-1/2} = 1$ modulo p, et écrivons $a = z^m$, on a $z^{m(p-1)/2} = 1$ donc il existe un nombre entier k' tel que $m(p-1) = 2k'(p-1)$ donc m est pair, $m = 2m'$, et $a = (zm')^2$.

Corollaire 3 du théorème 12 : si p est congru à 1 modulo 4, le nombre -1 est un résidu quadratique.

En effet $(-1)^{p-1/2} = 1$.

De là résulte le beau théorème d'arithmétique conjecturé (peut-être démontré) par Fermat et démontré par Euler (preuve publiée à l'appuis) : tout nombre premier p de la forme $4m + 1$ est diviseur d'un nombre de la forme $x^2 + 1$ (donc de la forme $a^2 + b^2$ avec a et b premiers entr eux).

Pour démontrer que p lui-même est une somme de deux carrés (forcément premiers entre eux), comme l'avait conjecturé Fermat et comme l'a établi Euler, nous utiliserons les entiers de Gauss $a + ib$, avec $a, b \in \mathbb{Z}$; ce qui sera une de nos motivations pour la toute dernière partie du cours sur les *extensions de corps.*

Remarque : on définit le symbole de Legendre $(\frac{a}{n})$ lorsque $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$ est un nombre impair, non nécessairement premier, et que a est un nombre

entier premier avec n par la formule suivante

$$(\frac{a}{n}) = (\frac{a}{p_1})^{\alpha_1}(\frac{a}{p_2})^{\alpha_2}...(\frac{a}{p_m})^{\alpha_m} \tag{38}$$

Le symbole est en général étendu en prenant 0 si a n'est pas premier avec n. Lorsque $a \equiv b \quad mod.n$ on a $(\frac{a}{n}) = (\frac{b}{n})$. Cela vient du fait que si a est congru à b modulo n, alors a congru à b modulo p pour tout diviseur premier de n. Attention : si a est résidu quadratique modulo n le symbole de Legendre ainsi défini vaut $+1$, mais la réciproque est fausse. Par exemple si $n = p^2$ est le carré d'un nombre premier impair, le symbole vaut toujours $+1$ alors que (exercice) a est résidu quadratique modulo p^2 si et seulement si a est résidu quadratique modulo p (i.e. si $(\frac{a}{p}) = +1$).

Le point de départ de la théorie moderne des nombres (selon A.Weil ou E.Hecke) est la *loi de réciprocité quadratique*, qui fut devinée par Euler, énoncée par Legendre et démontrée par Gauss (en 1796, à l'âge de 19 ans, puis publiée en 1801) ; cette loi dit que si a et n sont impairs et positifs, on a

$$(\frac{a}{n}) = (\frac{n}{a})(-1)^{(\frac{a-1}{2})(\frac{n-1}{2})}, \tag{39}$$

On ajoute les deux formules complémentaires suivantes, valables pour n impair :

$$(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}} \tag{40}$$

et

$$(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}. \tag{41}$$

Avec ces deux formules on a encore que

$$(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n}) \tag{42}$$

Exemple d'application : cherchons si 23 est résidu quadratique modulo 127. D'après la loi générale, c'est vrai si et seulement si 127 n'est pas résidu quadratique modulo 23, car $(a-1)/2 = 11$ et $(n-1)/2 = 63$, et ceci est équivalent au fait que $(\frac{12}{23}) = -1$ car $12 = 127 - 5 \times 23$. Mais par multiplicativité du symbole on a $(\frac{12}{23}) = (\frac{3}{23})$, qui vaut $-(\frac{23}{3})$, car $(3-1)/2 = 1$ et $(23-1)/2 = 11$. Mais $(\frac{23}{3}) = (\frac{-1}{3})$ car $23 = -1 + 3 \times 8$, or -1 n'est pas résidu quadratique modulo 3, donc $(\frac{23}{3}) = -1$. Par conséquent 23 n'est pas un carré modulo 127. La méthode directe consiste à calculer 23^{63} modulo 127.

3 Anneaux et corps commutatifs

3.1 Les notions d'anneau et de corps

L'ensemble $\mathbb{Z}$ des entiers relatifs est muni de deux opérations fondamentales, l'addition et la multiplication, toutes deux associatives et commutatives, la multiplication étant distributive par rapport à l'addition. Les deux lois possèdent un élément neutre, qui est 0 pour l'addition, et 1 pour la multiplication. Chaque entier relatif a possède un inverse pour l'addition, c'est-à-dire qu'il existe a' dans $\mathbb{Z}$ avec $a + a' = 0$, c'est $a' = -a$, mais ceci est faux pour la multiplication : par exemple 0 n'a pas d'inverse, mais même 2 n'en a pas. En fait seuls $+1$ et -1 ont un inverse.

de même on a vu que quelque soit $n \in \mathbb{N}^*$, les lois + et $\times$ de Z induisent des lois + et $\times$ sur l'ensemble des classes de congruence $\mathbb{Z}/n\mathbb{Z}$, avec les mêmes éléments neutres 0,1. On peut donc faire de l'algèbre modulo n. Les mêmes règles de calcul s'appliquent, associativité et commutativité des deux lois, distributivité de la multiplication par rapport à l'addition. Là encore tous les éléments sont inversibles pour la loi + mais pas pour la loi $\times$. Les éléments inversibles forment le groupe $R(n)$. Seulement si $n = p$ est un nombre premier tous les éléments sauf 0 ont un inverse pour la multiplication.

De même les matrices carrées dans $M_n(\mathbb{R})$ (ou avec des coefficients dans $\mathbb{Z}, \mathbb{Q}, \mathbb{C}, ...$) peuvent être ajoutées et multipliées, toujours avec associativité, et distributivité, et commutativité de l'addition ; cependant la commutativité est fausse pour la multiplication dès que n est supérieur à 2. Il y a un 0, élément neutre pour l'addition et un $1 = 1_n$, élément neutre pour la multiplication. Comme dans le cas des entiers relatifs, tout élément est inversible pour l'addition mais certains éléments ne sont pas inversibles pour la multiplication. En fait les éléments inversibles forment le groupe GL_n.

Un cadre algébrique commun englobe ces exemples :

Définition : Soit A un ensemble muni de deux éléments particuliers 0 et 1 et de deux lois de composition interne, notées + et $\times$ (appelées respectivement addition ou somme et multiplication ou produit) ; on dit que A est un *anneau* si :
(i) $(A, 0, +)$ est un groupe commutatif ;
(ii)la loi $\times$ est associative, et distributive par rapport à l'addition, i.e. $\forall a, b, c \in A, \quad a(b + c) = ab + ac, \quad (b + c)a = (ba + ca$;
(iii) 1 est un élément neutre pour la loi $\times$.

Remarques : 1) certains auteurs n'imposent pas l'existence de l'unité multi-

plicative 1 ; dans ce cas nous dirons que A est un *pseudo-anneau*. 2) Lorsque plusieurs anneaux entre en jeu, on doit distinguer les différents éléments neutres, en notant 0_A et 1_A par exemple, et les différentes lois, par exemple en les notant $\sigma, \sigma', ...$ et $\mu, \mu', ...$, ou encore $+_A$ et $\times_A$.

On dit que l'anneau A est *commutatif* (là on ne dit pas abélien), si la multiplication est commutative, i.e. si $\forall a, b \in A, \quad ab = ba$.

Par exemple Z est commutatif, Z/nZ aussi, mais pas $M_n(R)$.

Définitions : 1) une partie B d'un anneau A est un *sous-anneau* de A si elle est elle-même un anneau pour les opération somme et produit de A.
2) Une application $f : A \to A'$ d'un anneau A dans un anneau A' est un morphisme d'anneaux si c'est un morphisme de groupes additifs (pour les lois $+$) et si en plus on a $f(1) = 1'$ et $\forall a, b \in A, \quad f(ab) = f(a)f(b)$.
Un *isomorphisme* d'anneau de A sur A' est un morphisme bijectif ; alors son inverse est un morphisme (exercice).
3) Si A_1, A_2 sont deux anneaux, on définit *l'anneau produit* comme étant l'ensemble $A_1 \times A_2$ des paires (a_1, a_2) où $a_1 \in A_1$ et $a_2 \in A_2$, avec les lois évidentes :

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2), \quad (a_1, a_2) \times (b_1, b_2) = (a_1 \times b_1, a_2 \times b_2), \tag{43}$$

et les éléments neutres évidents $0 = (0_1, 0_2)$, $1 = (1_1, 1_2)$.
Exercice : c'est bien un anneau.

Exemple : l'anneau produit $Z/nZ \times Z/mZ$.

Théorème 1 : si n et m sont des entiers premiers entre eux, l'application naturelle de Z/nmZ dans $Z/NZ \times Z/mZ$ est un isomorphisme d'anneaux.

Démonstration : cette application naturelle est celle du théorème 3 du chapitre sur les groupes. Elle préserve évidemment le produit, et nous avons déjà démontré qu'elle est bijective.

Comme on le voit le lemme chinois nous poursuit en s'affinant.

Définition : soit A un anneau ; l'ensemble des éléments de A qui admettent un inverse pour la multiplication est noté $A^\times$.
Cet ensemble forme évidemment un groupe dont l'unité est 1_A.
La notation A^* désigne le complémentaire $A \backslash \{0\}$ de 0 dans A ; en général

$A^\times \neq A^*$.

Exemples : $R(n)$ pour l'anneau Z/nZ ; GL_n pour l'anneau M_n.

Proposition 1 : $(A_1 \times A_2)^\times = (A_1)^\times \times (A_2)^\times$.

Pour $R(n)$ et $R(m)$ avec $(m,n) = 1$ cela redonne $\varphi(mn) = \varphi(m)\varphi(n)$.

Théorème 2 : soit $N \geq 1$ un nombre naturel sans facteur carré, et n un nombre entier premier avec $\varphi(N)$; alors l'application $f(x) = x^n$ donne une bijection de l'anneau $A_N = Z/NZ$ dans lui même. La bijection inverse est donnée par $f'(x) = x^{n'}$ où n' est un inverse de n modulo $\varphi(q)$.

Démonstration : Notons que f et f' sont des homomorphismes d'anneau. D'après le théorème précédent, il existe un isomorphisme d'anneau ψ de A_N sur le produit des A_p où p décrit l'ensemble des facteurs premiers de N. Et sur chaque facteur f (resp. f') induit un morphisme donné par la même formule $x \mapsto x^n$ (resp. $x \mapsto x^n$). Il suffit donc d'établir le résultat pour A_p avec p premier, mais si $nn' = 1 + k\varphi(N)$ et si $N = pN'$, pour tout $x \in \mathbb{Z}$ on a

$$(x^n)^{n'} = x^{nn'} = x(x^{\varphi(N)})^k = x(x^{k(p-1)\varphi(N')} = x(x^{p-1})^{k\varphi(N')}, \qquad (44)$$

qui vaut 0 modulo p si x est congru à 0 modulo p et qui vaut x si x n'est pas congru à 0 modulo p d'après le petit théorème de Fermat.

Attention : ce résultat est faux dans l'anneau $A_q = \mathbb{Z}/q\mathbb{Z}$, lorsque $q = p^\alpha$ est une puissance d'un nombre premier, pour n premier avec $\varphi(q) = p^{\alpha-1}(p-1)$ tel que $n\alpha \geq \alpha + n$. En effet, on a dans ce cas $f(p^{\alpha-1}) = 0$ mais $p^{\alpha-1} \neq 0$. Par exemple, dans A_4, avec $n = 3$, on a $2^3 \equiv 0$, mais $2 \neq 0 \quad mod.4$, ou dans A_9, avec $n = 5$, on a $3^5 \equiv 0$, mais $3 \neq 0 \quad mod.9$.

Définition : un *corps* est un anneau où tout élément autre que 0 est inversible pour la multiplication.
Un anneau est un corps si et seulement si $A^\times = A^*$.
Un corps commutatif est un corps qui est commutatif en tant qu'anneau.
Exemples : $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Exemple : lorsque p est un nombre premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps fini commutatif, que l'on note $\mathbb{F}_p$.
En fait si N est un nombre entier l'anneau $\mathbb{Z}/N\mathbb{Z}$ est un corps si et seulement si N est premier.

3.2 L'anneau des polynômes $A[X]$.

Définition : soit A un anneau commutatif, et X un symbole ; un polynôme $P(X)$ à coefficients dans A est une somme finie $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$. Mais on décide que deux écritures dont tous les coefficients non-nuls coïncident définissent le même polynôme, par exemple $1.X + 5.X^3 = 1.X + 5.X^3 + 0.X^7$.
Pour simplifier l'écriture, on convient aussi d'écrire $X^0 = 1$, $X^k = 1.X^k$ et $-aX^k = (-a)X^k$.
L'écriture avec des puissances de X est donc une manière de coder une suite infinie $(a_0, a_1, ..., a_k, ...)$ dans A dont tous les termes sont nuls à partir d'un certain rang. Le plus grand n tel que $a_n \neq 0$ s'appelle le *degré* de P, et il est noté $deg(P)$. Ceci ne définit pas de degré pour le polynôme 0, dit polynôme nul ; on convient que son degré est $-\infty$.
L'addition des polynôme n'est rien d'autre que l'addition terme à terme des coefficients : si $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ et $Q(X) = b_0 + b_1X + b_2X^2 + ... + b_mX^m$ sont deux polynômes, on définit

$$(P+Q)(X) = (a_0+b_0) + (a_1+b_1)X + (a_2+b_2)X^2 + ... + (a_N+b_N)X^N \quad (45)$$

où $N = sup(n, m)$ est le maximum de n et m et où les coefficients de P ou Q ont été complétés par des zéros pour atteindre N.
Si $deg(P) \neq deg(Q)$, on a $P + Q \neq 0$ et $deg(P + Q) = sup(deg(P), deg(Q))$.
Si $deg(P) = deg(Q)$ on a $deg(P + Q) \leq sup(deg(P), deg(Q))$.
Ce qui justifie la notation $P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n$ est l'expression de la multiplication des polynômes :

$$(PQ)(X) = (a_0b_0) + (a_0b_1 + a_1b_0)X + (a_0b_2 + a_1b_1 + a_2b_0)X^2 + ...; \quad (46)$$

qui se déduit formellement de la règle $X^kX^l = X^{k+l}$.
On a $deg(PQ) \leq deg(P)+deg(Q)$ (règle qui marche bien avec $deg(0) = -\infty$).

L'élément neutre pour l'addition est le polynôme nul. L'élément neutre pour la multiplication est 1, de degré 0.

Proposition 2 : muni des lois + et $\times$, $A[X]$ est un anneau commutatif.

Définition : si a est un élément de A on note $P(a)$ l'élément de A en substituant a à X dans $P(X)$, c'est-à-dire $P(a) = a_0 + a_1a + a_2a^2 + ... + a_na^n$.

On dit que a est une *racine* de P si $P(a) = 0$.

Proposition 3 : si a est une racine de P, il existe un polynôme $Q(X)$ de degré égal à $deg(P) - 1$ tel que $P(X) = (X - a)Q(x)$.

La preuve utilise le résultat suivant, qui se vérifie facilement :

Lemme 1 : pour tout entier naturel $n \geq 1$ on a

$$X^n - a^n = (X - a)(X^{n-1} + aX^{n-2} + ... + a^{n-2}X + a^{n-1}). \qquad (47)$$

Démonstration de la proposition 3 : comme $P(a) = 0$ on a $P(X) = P(X) - P(a) = a_n(X^n - a^n + ... + a_1(X - a)$, et $X - a$ se met en facteur d'après le lemme.

Définition : un anneau A est dit *intègre* si quelque soit a, b différents de 0 on a $ab \neq 0$. Par exemple un corps est intègre, mais aussi $\mathbb{Z}$ qui n'est pas un corps est intègre.

Remarque : il est facile de montrer que tout anneau intègre commutatif est sous-anneau d'un corps commutatif. Exemple : $\mathbb{Z} \subset \mathbb{Q}$.

Théorème 3 : si A est un anneau commutatif intègre un polynôme $P(X)$ de degré $n \geq 0$ n'a pas plus de n racines.

Démonstration : elle se fait par récurrence sur n. Supposons le théorème établi pour $0 \leq m < n$ et considérons $P(X) \in A[X]$ de degré n ; si a est une racine de P, on écrit $P(X) = (X - a)Q(X)$ avec $deg(Q) = n - 1$. Soit $b \neq a$, l'équation $(b - a)Q(b) = 0$ implique $Q(b) = 0$, donc toute racine b de Q différente de a est une racine de Q. En vertu de l'hypothèse de récurrence, il ne peut donc y avoir plus de $n - 1$.

Attention : ce résultat est en général faux dans un anneau non-intègre. Exemple : dans $Z/8Z$ le polynôme $X^2 - 1$ a quatre racines, qui sont $1, 3, 5, 7$. Ce théorème est également faux dans les corps non-commutatifs, dits "corps gauches".

De là, comme on l'a expliqué dans le chapitre précédent sur les groupes abéliens finis, on déduit le résultat attendu suivant :
Théorème 4 : soit A un anneau intègre commutatif et G un sous-groupe fini du groupe multiplicatif A^* ; alors G est cyclique.

Proposition 4 : si A est intègre $A[X]$ l'est.

En effet soit $P(X) = a_n X^n + ... + a_0$ et $Q(X) = b_m X^m + ... + b_0$ deux polynômes non nuls de degrés n et m respectivement, le terme de plus haut degré de PQ est $a_n b_m X^{m+n}$ qui n'est pas nul puisque $a_n \neq 0$ et $b_m \neq 0$ et que A est intègre.

Attention, dans $\mathbb{Z}[X]$, comme dans la plupart des anneaux la division euclidienne n'existe pas.

3.3 Applications en cryptographie. Méthode RSA.

Un problème en cryptographie est d'envoyer des messages secrets à ses amis : les correspondant doivent pouvoir encoder et décoder facilement les messages sans que les espions puissent les déchiffrer.
L'alphabet X qui sert à écrire les messages comporte un nombre fini N de symboles élémentaires. On peut donc l'assimiler à l'ensemble $\mathbb{Z}/N\mathbb{Z}$ des nombres entiers modulo N. On peut même convenir que le message tout entier est contenu dans un seul caractère, ce qui est vraisemblable si N est assez grand ou si le message est juste "oui" ou "non".

L'idée des codes à *clés publiques* est que l'alphabet est connu, ainsi que l'encodage, mais pas le décodage.

Voici le principe : à un correspondant A est attribuée une bijection $f_A : X \to X$; c'est son code personnel, appelé aussi sa *clé publique*, de plus A (et lui seul) connaît l'inverse f_A^{-1} ; c'est sa *clé secrète*. Le principe est que les autres personnes, même s'ils connaissent la formule de f_A, n'arrivent pas à calculer f_A^{-1} en un temps raisonnable. On suppose donc que X et les codes f_i de tous les citoyens abonnés $i \in I$ sont dans un annuaire. Maintenant, si A veut envoyer le message $m \in X$ à B, il lui communique $m' = f_B \circ f_A^{-1}(m) = f_{BA}(m)$, et B, pour lire le message, c'est-à-dire retrouver m, n'a qu'à calculer $f_A \circ f_B^{-1}(m') = f_{AB}(m') = m$.

Remarque : un gros avantage de cette méthode est que B peut facilement vérifier que le message provient bien de A et pas d'un pirate. En effet, il suffit à B d'envoyer un message à A et de voir si A est capable de le retourner à l'identique, car pour arriver à le faire convenablement A doit se servir de sa clé secrète.
Notez que les codes doivent être attribués par un administrateur "neutre", d'où un problème d'autorité évident, et des risques d'abus de pouvoir.

Dans le cas particulier nommé RSA, l'entier N est supposé être le produit de plusieurs nombres premiers très grands, aucun n'ayant de multiplicité supérieure à 1, et les bijections f_i sont de la forme

$$f_i(a) = a^{n_i}, \tag{48}$$

où n_i est un nombre entier premier avec $\varphi(N)$; si bien que la clé publique numéro i est le nombre n_i. La clé privée, elle, est donnée par un entier n_i' tel que $n_i' n_i \equiv 1 \quad mod.\varphi(N)$. Élever un nombre modulo N à la puissance n_i' est bien l'inverse de f_i, en vertu du théorème 2 ci-dessus.

Attention : il faut que $\varphi(N)$ reste secret pour tout le monde, sauf pour l'administrateur. En effet, si ce nombre est connu, un algorithme d'Euclide entre lui et n_i fournit immédiatement la clé secrète n_i'.

Dans la pratique N est le produit de deux nombres premiers distincts, p et q. Alors $\varphi(N) = (p-1)(q-1)$. Et la connaissance de $\varphi(N)$ équivaut à celle de la factorisation $N = pq$. En effet, il est évident que connaissant p et q on en déduit $\varphi(N)$, et réciproquement, si on a N et $\varphi(N)$, on en déduit $p + q = N + 1 - \varphi(N)$ d'où p et q grâce à la formule donnant les racines de l'équation du deuxième degré $X^2 - (N + 1 - \varphi(N))X + N = 0$.

L'inviolabilité des secrets RSA repose dès lors sur la difficulté de la factorisation en nombres premiers d'un nombre trop grand. Effectivement, à l'heure actuelle aucun algorithme rapide n'est connu pour résoudre ce problème. Cependant, il n'est pas démontré qu'un tel algorithme n'existe pas, et il se peut aussi qu'il existe des algorithmes donnant des solutions dans beaucoup de cas sans les donner toujours. De plus il est démontré que les "ordinateurs quantiques", s'ils étaient réalisés, seraient capable de résoudre ce problème en temps rapide.

Pour faire fonctionner RSA il faut savoir engendrer des grands nombres premiers. Le principe est de tirer n au hasard et de décider si oui ou non n est premier. Cette décision repose sur des tests de primalités.

Critères de primalité. La méthode la plus sure pour savoir si n est premier est de considérer les uns après les autres les nombres $a \leq \sqrt{n}$ et de regarder s'ils divisent n ou non.
Des méthodes plus rapides ont été recherchées. La plus connue consiste à faire appel au petit théorème de Fermat : si n est premier, alors quelque soit

a, avec $0 < a < n$, premier avec n, on a $a^{n-1} \equiv 1 \quad mod.n$.
Cela permet d'éliminer rapidement beaucoup de candidats n à la primalité. Par exemple ???.
Cependant, ce test n'est pas sur. En effet il se peut que pour tout a premier avec n on ait $a^{n-1} \equiv 1 \quad mod.n$ sans que n soit premier.
Supposons que n est sans facteur carré, alors $\varphi(n)$ est un produit de nombres $p-1$ distincts, et supposons que chaque facteur $p-1$ de $\varphi(n)$ divise $n-1$; cela donne un contre-exemple à la réciproque du petit théorème de Fermat. En effet, si a est premier avec n, il est premier avec chaque diviseur premier p de n, donc $a^{p-1} \equiv 1 \quad mod.p$. Alors le lemme chinois entraîne que pour chaque p on a $a^{p-1} \equiv 1 \quad mod.n$. Comme $p-1$ divise $n-1$ on en déduit que $a^{n-1} \equiv 1 \quad mod.n$.
Un tel nombre n s'appelle un *nombre de Carmichael*. Exemple : $n = 561$ est un nombre de Carmichael. En effet $561 = 3.11.17$, donc $\varphi(561) = 2.10.16 = 2^5.5$, et $n - 1 = 560 = 2^4.5.7$.
Par contre il est vrai que $a^{n-1} \equiv 1 \quad mod.n$ pour tout a entre 1 et $n-1$ entraîne que n est premier, car dans ce cas tous les nombres plus petit que n ont un inverse modulo n donc sont premiers avec n.
Remarque : il suffirait de prendre ici les nombres a premiers et inférieurs à la racine carrée de n. Déterminer si $a < n$ est premier avec n repose sur l'algorithme d'Euclide qui est plutôt rapide, mais le faire pour tous les entiers avant $\sqrt{n}$ est bien trop long.
Cependant il est intéressant, au moins théoriquement, de chercher des critères surs ne portant que sur les éléments de $R(n)$.

D'où l'intérêt du test de Rabin-Miller :
.....

Remarque sur le coût des calculs. La complexité d'un nombre entier naturel n en base b est $log(n)/log(b)$, qui est approximativement le nombre de chiffres pour écrire n en base b.
L'addition de n, m a un coût approximatif en $O(log(sup(n,m)))$. La multiplication en $O(log(sup(n,m))^2)$. Pareil pour la division euclidienne.
Pour l'algorithme d'Euclide cela donne $O(log(sup(n,m))^3)$.
Pour l'exponentielle m^n, on a $logm$ multiplications d'où $O(log(sup(n,m))^2 log(m))$ et pour l'exponentielle $m^n \quad mod.N$ on trouve $O(log(sup(n,m))^2 log(m) log(N)^2)$.
Répéter l'opération pour tous les entiers $a < k$ met un k en facteur et là c'est trop.

.....

3.4 Divisibilité dans $K[X]$

Dans un corps il y a une méthode encore plus naturelle pour établir le théorème 3, en s'appuyant sur la division euclidienne :

Théorème 5 : soit K un corps commutatif, P, Q deux éléments de $K[X]$, avec $Q \neq 0$, alors il existe une unique paire S, R d'éléments de $K[X]$, telle que $P = SQ + R$ et que $deg(R) < deg(Q)$.

Démonstration : L'unicité est facile ; en effet si $S_1Q + R_1 = S_2Q + R_2$ on a $R_1 - R_2 = (S_1 - S_2)Q$, mais si $S_1 \neq S_2$ le degré de $(S_1 - S_2)Q$ est supérieur à m, ce qui ne se peut pas. Pour l'existence : si le degré n de P est strictement inférieur au degré m de Q le résultat est évident ; sinon on raisonne par récurrence sur $n \geq m$. Supposons le théorème vrai pour les degrés inférieurs à $n - 1$, considérons les termes de plus haut degré a_nX^n, b_mX^m de P et Q respectivement, et posons

$$P_1(X) = P(X) - a_n b_m^{-1} X^{n-m} Q(X); \tag{49}$$

alors on a $deg(P_1) < n$ donc il existe S_1, R_1 avec $deg(R_1) < m$ tels que $P_1 = S_1Q + R_1$, d'où

$$P(X) = (S_1(X) + a_n b_m^{-1} X^{n-m})Q(X) + R_1(X). \tag{50}$$

On dit que l'écriture $P = SQ + R$ est la *division euclidienne* de P par Q, et que S et R sont respectivement le *quotient* et le *reste* de cette division.

Re-démontrons le théorème 3 dans le cas où $A = K$ est un corps : la division euclidienne de P par $X - a$ donne $P(X) = S(S)(X - a) + c$, où c est une constante, un polynôme de degré 0 car le degré de $X - a$ est 1, et si $P(a) = 0$ on a $c = 0$ donc $X - a$ divise $P(X)$.

De l'existence de la division euclidienne dans l'anneau $K[X]$ on déduit les résultats analogues à ceux qu'on avait démontré pour Z à partir de la division euclidienne des nombres entiers :

Corollaire 1 : un sous-ensemble non-vide de $K[X]$ qui est stable par soustraction est de la forme $P(X)K[X]$.

Corollaire 2 : un pgcd $D(X)$ de P et Q est divisé par tout diviseur commun de P et Q, et il existe des polynômes $U(X), V(X)$ tels que $D(X) = U(X)P(X) + V(X)Q(X)$.

C'est-à-dire que le théorème de Bézout est vrai pour les polynômes sur un corps commutatif.

Définition : un polynôme P est dit *irréductible* (ou *premier*) s'il est de degré supérieur ou égal à 1 et si ses diviseurs sont les constantes non-nulles, ou lui même à un facteur constant près, c'est-à-dire a ou bP, avec $a, b \in K^*$.

Corollaire 3 : tout polynôme s'écrit comme produit de polynômes irréductibles, de façon unique à permutation près et à multiplication près par des éléments non nuls de K.

Exemples de Polynomes irréductibles. Cas de R, C, Q, F_p.

3.5 Extensions de corps. Applications

Pour un anneau A, définition de *module à gauche* (resp. à droite) sur un anneau. Définition d'idéal à droite (resp. à gauche). Congruence modulo un idéal. Ensemble quotient. Cas des idéaux bilatères. Anneau quotient.
Exemples d'idéaux de $A[X]$, anneaux quotients.
Définition d'idéal principal.
Cas commutatif. Exemple des Z/nZ.
Passage au quotient des morphismes, exemples.

Idéal premier, idéal maximal. Corps quotient.

Construction directe des corps finis F_q, pour $q = p^n$.
Description comme quotient de $F_p[X]$ par la relation $X^q = X$.

Construction directe de $\mathbb{Q}[i]$, ou de $\mathbb{Q}[\zeta]$ avec $\zeta^n = 1$.

Entiers de Gauss, $\mathbb{Z}[i]$: application aux sommes de carrés, Fermat, Euler.

Triangles de Pythagore.

Extensions finies de $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$.

Indications d'applications en Arithmétique.