8.12. **Solutions générales.** Considérons l'équation $ax + by = c$, où a, b, c sont des entiers non-zéro. Par un corollaire du théorème de Bézout, il existe une solution entière si $d := \mathrm{pgcd}(a, b)|c$. Supposons ce cas. Alors il existe deux entiers a', b' tels que $a = a'd$, $b = b'd$. On a donc $ab' = a'b$ et $\mathrm{pgcd}(a', b') = 1$. Par l'algorithme de Bézout nous pouvons obtenir une solution entière particulière, disons $ax_0 + by_0 = c$.

Proposition 8.1. *Considérons l'équation $aX + bY = c$, où a, b, c sont des entiers, tel que $d := \mathrm{pgcd}(a, b)|c$. Il y a des entiers a' et b' tels que $a = a'd$, $b = b'd$. Supposons (x_0, y_0) est une solution entière particulière.*

La paire (x_1, y_1) de deux entiers est aussi une solution entière de cette équation si et seulement s'il existe un entier t tel que

$$x_1 = x_0 + tb',\ y_1 = y_0 - ta'.$$

Démonstration. (i) Une direction : la paire $(x_0 + tb', y_0 - ta')$ est aussi une solution :

$$a(x_0 + tb') + b(y_0 - ta') = (ax_0 + by_0) + t(ab' - a'b) = c + 0 = c.$$

(ii) L'autre direction : *Supposons* (x_1, y_1) est aussi une solution entière, alors

$$ax_0 + by_0 = c = ax_1 + by_1,$$

et donc $a(x_1 - x_0) = -b(y_1 - y_0)$ et

$$da'(x_1 - x_0) = -db'(y_1 - y_0).$$

Parce que $d \neq 0$, il suit

$$a'(x_1 - x_0) = -b'(y_1 - y_0).$$

Évidemment b' divise $-b'(y_1 - y_0)$, donc b' divise aussi $a'(x_1 - x_0)$. On a $\mathrm{pgcd}(a', b') = 1$ (exercice : montrer ça), donc par thm.8.9(i) il suit

$$b'|(x_1 - x_0).$$

Par définition, il existe un entier t tel que $tb' = x_1 - x_0$, ou on obtient *en effet* que

$$x_1 = x_0 + tb'.$$

Puis, en multipliant des deux côté par a' de $tb' = x_1 - x_0$ on obtient :

$$a'tb' = a'(x_1 - x_0) = -b'(y_1 - y_0)$$

et, parce que $b' \neq 0$,

$$a't = -(y_1 - y_0).$$

Il suit finalement qu'on a aussi

$$y_1 = y_0 - ta'.$$

□

Remarque. Pour trouver les solutions entières *non-négatives* de $aX + bY = c$, il faut déterminer les $t \in \mathbb{Z}$, dans la proposition, pour lesquelles, simultanément,

$$x_1 = x_0 + tb' \geq 0 \quad \text{et} \quad y_1 = y_0 - ta' \geq 0.$$

Possiblement de tels t n'existent pas, ou on en a plusieurs. Il suit un exemple.

8.12.1. *Problème :* Un marchand vend deux types de T-shirts, l'un avec un C, l'autre avec un O. Celui avec un C coûte \$33 chacun, et celui avec un O coûte \$29 chacun. Dans un après-midi il a vendu pour \$508 de marchandise. Combien de T-shirts a-t-il vendu ?

Solution : Si u le nombre de T-shirts de type C vendus, et v le nombre de T-shirts de type O vendus :

$$33u + 29v = 508$$

(ici $u \in \mathbb{N}$ et $v \in \mathbb{N}$ certainement). À trouver $u + v$.

D'abord, trouvons une solution entière particulière de l'équation $33x + 29y = 508$, avec la méthode de Bézout :

$$\begin{aligned} 1 \cdot 33 + 0 \cdot 29 &= 33 \\ 0 \cdot 33 + 1 \cdot 29 &= 29 \\ 1 \cdot 33 + (-1) \cdot 29 &= 4 \ (= 33 - 29) \\ (-7) \cdot 33 + (8) \cdot 29 &= 1 \ (= 29 - 7 \cdot 4); \end{aligned}$$

en particulier $\text{pgcd}(33, 29) = 1$. On multiplie par 508

$$(-7 \cdot 508) \cdot 33 + (8 \cdot 508) \cdot 29 = 508.$$

Ou $x = -7 \cdot 508 = -3556$ et $y = (8 \cdot 508) = 4064$ est une solution particulière de l'équation.

Mais ici $x < 0$, cette solution n'est pas ce qu'on veut ! Quelles sont les autres solutions ?

La solution générale est : Chaque autre paire de solutions entières de l'équation $33x+29y = 508$ est de la forme (la preuve suivra) $x' = -3556 + 29 \cdot a$ et $y' = 4064 - 33 \cdot a$ où $a \in \mathbb{Z}$.

Nous chercons une solution positive, c.-à-d. cherchons les $a \in \mathbb{Z}$ tel que

$$x' = -3556 + 29a \geq 0$$

$$y' = 4064 - 33a \geq 0$$

ou

$$a \geq \frac{3556}{29} = 122.62....$$

$$a \leq \frac{4064}{33} = 123.141....$$

Donc $a = 123$ est la *seule* possibilité ou $x' \geq 0$ et $y' \geq 0$! Nous pouvons conclure

$$u = -3556 + 123 \cdot 29 = 11 \text{ et } v = 4064 - 123 \cdot 33 = 5.$$

Le vendeur a donc vendu 11 T-shirts de type C et 5 T-shirts de type O, et en total il y a vendu 16 T-shirts. □

Montrons encore : "Chaque autre paire de solutions entières est de la forme $x' = -3556 + a \cdot 29$ et $y' = 4064 - a \cdot 33$ où $a \in \mathbb{Z}$."

Démonstration. On a $(-3556) \cdot 33 + (4064) \cdot 29 = 508$. Si aussi $x' \cdot 33 + y' \cdot 29 = 508$, alors

$$\begin{aligned} x' \cdot 33 + y' \cdot 29 &= (-3556) \cdot 33 + (4064) \cdot 29 \\ (x' + 3556) \cdot 33 &= (-y' + 4064) \cdot 29. \end{aligned}$$

En particulier $29|((x' + 3556) \cdot 33)$. Parce que $\text{pgcd}(33, 29) = 1$ ou parce que 29 est premier, il suit (par un cor. du thm. de Bézout, thm. 8.9)

$$29|(x' + 3556),$$

c.-à.d. il existe en entier a tel que $29a = x' + 3556$, ou

$$x' = -3556 + a \cdot 29.$$

Et $a \cdot 29 \cdot 33 = (x' + 3556) \cdot 33 = -(y' - 4064) \cdot 29$, donc

$$y' = 4064 - a \cdot 33.$$

□

8.12.2. *Problème.* Soient a, b, m des entiers, où $m > 0$. Soit $d := \text{pgcd}(a, m)$. Il y a des entiers a' et m' tels que $a = a'd$, $m = m'd$.

Considérons l'équation

$$aX \equiv_m b.$$

Supposons $x_0 \in \mathbb{Z}$ est une solution entière particulière, c.-à-d., $ax_0 \equiv_m b$.

Montrer en utilisant prop. 8.1 : L'entier $x_1 \in \mathbb{Z}$ est aussi une solution entière de cette équation si et seulement s'il existe un entier t tel que

$$x_1 = x_0 + tm'.$$

Pour trouver des solutions positives, il faut trouver les t tel que $x_1 = x_0 + tm' > 0$.

8.13. **Quelques problèmes résolus.**

8.13.1. *À montrer.* Pour chaque nombre naturel n le nombre

$$4^{n+2} + 5^{2n+1}$$

est divisible pas 21.

Solution : Au moins c'est vrae si $n = 0$: $21|21$; et si $n = 1$ car $189 = 9 \cdot 21$.

Calculons modulo 21 :

$$\begin{aligned} 4^{n+2} + 5^{2n+1} &\equiv_{21} 4^{n+2} + 25^n \cdot 5 \\ &\equiv_{21} (4^n \cdot 4^2) + 4^n \cdot 5 \\ &\equiv_{21} 4^n(16+5) \\ &\equiv_{21} 4^n \cdot 21 \\ &\equiv_{21} 0 \end{aligned}$$

(parce que $5^{2n+1} = 5^{2n} \cdot 5^1 = (25)^n \cdot 5$ et $25 \equiv_{21} 4$). Conclusion : 21 divise $4^{n+2} + 5^{2n+1}$. □

8.13.2. *Le petit théorème de Fermat.* [17] En calculant les hautes puissances modulo un nombre premier, un théorème de Fermat peut bien aider.

Théorème 8.14 (Fermat)**.** *Soit p un nombre premier et a un entier. Alors*

$$a^p \equiv_p a.$$

Nous allons donner la preuve d'Euler plus tard dans le cours, en utilisant induction.

Pour vous c'est seulement une curiosité sans doute. Mais c'est à l'origin de beaucoup d'applications, par exemple pour une communication secure entres les banques.

Exemple 8.8. Le nombre 11 est premier. Vérifions un cas spécial du théorème de Fermat.

$$14^{11} \equiv_{11} 3^{11} \equiv_{11} 3^{2\cdot 5+1} \equiv_{11} (9)^5 \cdot 3 \equiv_{11} (-2)^5 \cdot 3 \equiv_{11} -32 \cdot 3 \equiv_{11} 1 \cdot 3 \equiv_{11} 3 \equiv_{11} 14.$$

En effet. Nous n'avions pas besoin de calculer 14^{11} et puis calculer le reste après division par 11. Le calcul modulaire est beaucoup plus agréable que le calcul ordinaire. Les nombres impliqué restent petits ! Et ce théorème aide beaucoup pour calculer les hautes puissances.

8.13.3. *Problème :* Soit $n = (13^{27} + 199 \cdot 23 - 311) \cdot (2345 + 11^5)$. Quel est le dernier chiffre de n (dans la représentation décimale) ?

Solution : On a $n > 0$ donc nous cherchons le nombre $0 \leq r < 10$ tel que $n \equiv r \bmod 10$. Calculons modulo 10.

$$\begin{aligned} n &\equiv_{10} (3^{27} + 9 \cdot 3 - 1) \cdot (5 + 1^5) \\ &\equiv_{10} ((3^2)^{13} \cdot 3 + 27 - 1) \cdot (5+1) \\ &\equiv_{10} ((-1)^{13} \cdot 3 + 7 - 1) \cdot 6 \\ &\equiv_{10} (-3+6) \cdot 6 \\ &\equiv_{10} 18 \\ &\equiv_{10} 8 \end{aligned}$$

Conclusion : le dernier chiffre est 8.

17. Cette sous-section **n'est pas obligatoire** et ne fait pas partie de la matière examinée.

8.13.4. *Problème :* Soit $n = (13^{27} + 199 \cdot 23 - 311) \cdot (2345 + 11^5)$. Quel est le dernier chiffre de n dans la représentation hexadécimale ?

Solution : On a $n > 0$ donc nous cherchons le nombre $0 \leq r < 16$ tel que $n \equiv r \bmod 16$. Calculons modulo 16.

$$\begin{aligned}
n &\equiv_{16} ((-3)^{27} + 7 \cdot 7 - 7) \cdot (9 + (-5)^5) \\
&\equiv_{16} ((9)^{13} \cdot (-3) + 42) \cdot (9 + (25)^2 \cdot (-5)) \\
&\equiv_{16} ((81)^6 \cdot 9 \cdot (-3) + 10) \cdot (9 + (9)^2 \cdot (-5)) \\
&\equiv_{16} ((1)^6 \cdot (-27) + 10) \cdot (9 + (81) \cdot (-5)) \\
&\equiv_{16} (-17) \cdot (9 + (1) \cdot (-5)) \\
&\equiv_{16} (-1) \cdot (4) \\
&\equiv_{16} -4 \\
&\equiv_{16} 12
\end{aligned}$$

Donc le dernier chiffre est C(douze).

8.13.5. *Divisibilité par* $2, 3, 4, 5, 6, 8, 9, 10, 11, 12$. Soit N un nombre, disons $N = 765592314$.

Ce nombre est pair parce que son dernier chiffre 4 est pair. C'est un 3-multiple car la somme des chiffres $7 + 6 + 5 + 5 + 9 + 2 + 3 + 1 + 4 = 42$ est divisible par 3. Ce n'est pas un 4-multiple, car 14 n'est pas divisible par 4. N'est pas un 5-multiple, parce que le dernier chiffre 4 n'est pas divisible par 5. C'est un 6-multiple, parce que c'est un 2-multiple et un 3-multiple. Ce n'est pas un 8 multiple, car 314 n'est pas divisible par 8. N'est pas un 9-multiple, car la somme des chiffres 42 n'est pas divisible par 9. N'est pas divisible par 10 car le dernier chiffre n'est pas 0. N'est pas divisible par 11 car la somme alterné des chiffres $7 - 6 + 5 - 5 + 9 - 2 + 3 - 1 + 4 = 14$ n'est pas divisible par 11. N'est pas divisible par 12, car ce n'est pas divisible par 4.

Et si on écrit N sur une autre base, disons $m > 0$? Soit $N \in \mathbb{N}$ écrit sur la base m :

$$N = [c_s, c_{s-1}, \ldots, c_1, c_0]_m,$$

c.-à-d. $N = \sum_{i=0}^{s} c_i \cdot m^i$ et $0 \leq c_i < m$ pour chaque c_i.

(i) Soit $a|m$. Alors $a|N$ si et seulement si $a|c_0$. Cas spécial : $m|N$ si et seulement si $c_0 = 0$.
Il y a des généralisations, par exemple :
(i-bis) Soit $a|m^3$. Alors $a|N$ si et seulement si $a|[c_2c_1c_0]_m$.

(ii) Soit $a|(m-1)$. Alors $a|N$ si et seulement si a divise la somme des chiffres :

$$a|(c_s + c_{s-1} + \ldots + c_2 + c_1 + c_0) = \sum_{i=0}^{s} c_i..$$

(iii) Soit $a|(m+1)$. Alors $a|N$ si et seulement si a divise la somme alternée des chiffres :

$$(-1)^s c_s + \ldots - c_3 + c_2 - c_1 + c_0 = \sum_{i=0}^{s} (-1)^i c_i.$$

Démonstration. Une preuve de (iii) seulement. Donner une preuve pour les autres vous même. Remarquons d'abord qu'il existe un entier b tel que $ab = m+1$ ou $m = ab-1$. Donc modulo a : $m \equiv_a (-1)$ et

$$m^i \equiv_a (-1)^i.$$

On a $n = \sum_{i=0}^{s} c_i \cdot m^i$, donc modulo a :

$$n = \sum_{i=0}^{s} c_i \cdot m^i \equiv_a \sum_{i=0}^{s} c_i \cdot (-1)^i.$$

Alors n et la somme alternée de chiffres $\sum_{i=0}^{s}(-1)^i c_i$ ont le même reste modulo a : en particulier $a|n$ si et seulement si a divise $\sum_{i=0}^{s}(-1)^i c_i$. □

Exemple 8.9. Sur la base 16. Si $n = [A, 1, 5, 6, C, 1, 3, C]_{16}$, alors la somme des chiffres est $10 + 1 + 5 + 6 + 12 + 1 + 3 + 12 = 50$, la somme alternée des chiffres est $-10 + 1 - 5 + 6 - 12 + 1 - 3 + 12 = -10$.

On a $5|(16-1)$ et $3|(16-1)$. Donc $5|n$ si et seulement si $5|50$ (ce qui est le cas), et $3|n$ si et seulement si $3|50$ (ce qui n'est pas le cas).

Le dernier chiffre est C (douze), donc n n'est pas divisible par 16 ni par 8, mais n est divisible par 2 et 4.

On a $17|(16+1)$. Donc $17|n$ si et seulement si $17|-10$ (ce qui n'est pas le cas).

8.13.6. *Problème :* Soit $n = [A, 2, 9, 9, 2, 3, 5, 7, 8, 3, 4, 5, C, 1, 0]_{16}$. C'est quoi le reste si on divise n par 4096 ?

Réponse : On remarque que $4096 = 16^3$ et "donc" le reste est $[C, 1, 0]_{16} = 12 \cdot 16^2 + 16 = 3088$. Pourquoi ? □

8.13.7. *Problème :* Soit

$$m = [9, 2, 9, 9, 2, 3, 5, 7, 8, 3, 4, 5, 9, 1, 0]_{16}$$

et

$$q = [9, 2, 9, 9, 2, 3, 5, 7, 8, 3, 4, 5, 9, 1, 0]_{11}.$$

Montrer que $m - q$ est divisible par $16 - 11 = 5$.

Réponse : "Parce que" (pourquoi ?) : on a pour chaque i

$$(16^i - 11^i) \equiv_5 (1^i - 1^i) \equiv_5 0.$$

9. Relations d'équivalences

Il est naturel de classifier des choses et nous le faisons tout le temps. Les animaux sont classifiés dans plusieurs classes : les chiens, les chats, les oiseaux, les giraffes, etcetera. Les symbôles sont divisés dans les classes a,b,c, ...,z,1,2, ...*,&,*,(, ?,... Les symbôles A, a, a, $\mathbf{a}$, a ... sont tous dans la même classe "a".

Les nombres naturels sont de deux sortes : ceux qui sont pairs et ceux qui sont impairs. On considère Pair et Impair comme deux objets, et on dit des choses comme : Pair + Impair = Impair, Impair fois Impair est Impair. Pair et Impair ce comportent comme une sorte de nombres généralisés.

Nous avons un grand besoin de modéliser cet idée en termes d'ensembles. On le fait avec la notion de *relation d'équivalence*. Il ne faut pas avoir trop de peur de ça, c'est une abstraction d'une idée naturelle. Mais probablement ça prend du temps de s'habituer, un peu comme on s'est habitué à l'école primaire aux fractions. En fait, une fraction (ou un élément de $\mathbb{Q}$) est un exemple d'une classe d'équivalence. Aussi une bonne définition des nombres réels se fait par une relation d'équivalence (mais un peu trop compliqué pour notre cours).

Qu'est-ce qu'on veut ? Nous voulons diviser les éléments d'un ensemble fixé de notre intéresse, disons U, dans plusieurs classes (=sous-ensembles) non-vides, selon une classification peut-être. On veut :

- Chaque élément est classifié dans une classe ;
- On ne veut pas permettre à un élément d'appartenir à deux ou plus de classes différentes.

Ses classes forment les *éléments* d'un nouveau ensemble, $(U/\sim) \subset P(U)$, et on obtient une fonction surjective $\mathrm{C}\ell : U \to (U/\sim)$ (l'application *classification*) où $\mathrm{C}\ell(u)$ est l'*unique* classe qui contient u.

9.1. Une définition de relation d'équivalence.

Soit U un ensemble et $F(u_1, u_2)$ une fonction propositionnelle avec univers du discours $U \times U$. Nous allons écrire

$$\begin{aligned} u_1 \sim u_2, &\qquad \text{si } F(u_1, u_2) \text{ vrai ;} \\ u_1 \not\sim u_2, &\qquad \text{si } F(u_1, u_2) \text{ faux .} \end{aligned}$$

Définition 9.1. *Nous allons dire que $\sim$ (ou F) est* une relation d'équivalence *sur U si pour chaque u, v, w élements de U on a*

(i) $u \sim u$ (réflexive) ;

(ii) si $u \sim v$ alors $v \sim u$ (symétrique) ;

(iii) si $u \sim v$ et $v \sim w$ alors $u \sim w$ (transitive).

Dans ce cas nous allons dire que u est équivalent à *v si $u \sim v$.*

Remarque. À la place du symbole $\sim$, aussi autres symboles sont utilisés pour des relations d'équivalence, comme $\equiv$. Voir aussi [R, §6.5].

Dans la suite du section nous supposons que $\sim$ est une relation d'équivalence sur U.

9.2. **Classes d'équivalence.** Soit $u \in U$. Définissons sa *classe d'équivalence*

$$\mathrm{C}\ell(u) = \{v \in U |\ u \sim v\} \subseteq U.$$

Remarque. À la place d'utiliser $\mathrm{C}\ell(u)$ comme notation pour la classe d'équivalence de u, souvent une notation comme $\overline{u}$ est utilisée. Ou autres.

Chaque élément $u \in U$ est contenu dans sa propre classe d'équivalence $\mathrm{C}\ell(u)$ et si deux classes d'équivalence sont différentes, alors elles sont mêmes disjointes. En conséquence, chaque élément de U est contenu dans une *unique* classe d'équivalence. Ce sont des conséquence du lemme suivant.

Lemme 9.1. *Soient $u, v \in U$.*
(i) $u \in \mathrm{C}\ell(u)$;
(ii) $\mathrm{C}\ell(u) \cap \mathrm{C}\ell(v) \neq \emptyset$ si et seulement si $\mathrm{C}\ell(u) = \mathrm{C}\ell(v)$.

Démonstration. (i) $u \in \mathrm{C}\ell(u)$ parce que $u \sim u$ (par réflexivité).

(ii) Soit $w \in \mathrm{C}\ell(u) \cap \mathrm{C}\ell(v)$, c.-à-d., $u \sim w$ et $v \sim w$. Par symétrie aussi $w \sim u$ et $w \sim v$. Donc par transitivité on a aussi $u \sim v$, $v \sim u$. Si $x \in \mathrm{C}\ell(u)$ alors $u \sim x$ et $x \sim u$. Avec $u \sim v$ et transitivité il suit $x \sim v$ et $v \sim x$, ou $x \in \mathrm{C}\ell(v)$. Donc $\mathrm{C}\ell(u) \subseteq \mathrm{C}\ell(u) \cap \mathrm{C}\ell(v) \subseteq \mathrm{C}\ell(u)$. Il suit $\mathrm{C}\ell(u) = \mathrm{C}\ell(u) \cap \mathrm{C}\ell(v)$ et $\mathrm{C}\ell(u) = \mathrm{C}\ell(v)$. $\square$

9.3. **Ensemble des classes d'équivalence.** *Posons*

$$(U/\sim) := \{\mathrm{C}\ell(u) |\ u \in U\}$$

pour l'ensemble des classes d'équivalence différentes. C'est un ensemble important ! Aussi dans la vraie vie. Nous pouvons donc considérer chaque $\mathrm{C}\ell(u)$ comme sous-ensemble de U, comme élément de $P(U)$ ou comme élément de $U/\sim$.

Remarque. Pour beaucoup de relations d'équivalence l'ensemble $(U/\sim)$ a une notation particulière, et ses éléments sont notés de façon particulier aussi. Souvent on ne reconnaît plus tout de suite certains ensembles comme des "$U/\sim$ ", et ses éléments comme de type "$\mathrm{C}\ell(u)$". Et c'est bon comme ça.

Chaque élément $C \in (U/\sim)$ est par définition de la forme $C = \mathrm{C}\ell(u)$, pour un $u \in U$, mais un tel u n'est pas unique en général. Considérons $u_1, u_2 \in U$ alors

$$u_1 \sim u_2 \text{ si et seulement si } \ \mathrm{C}\ell(u_1) = \mathrm{C}\ell(u_2),$$

(égalité comme éléments de $U/\sim$ ou comme sous-ensembles de U).

Soient $C \neq C'$ deux éléments différents de $U/\sim$. Ce sont donc deux sous-ensembles différents de U. Mais le lemme 9.1 nous dit que ces deux ensembles sont mêmes disjoints !

9.4. **Partition par les classes d'équivalences.** Supposons l'ensemble U est fini. Alors le fait que chaque élément de U est dans un *unique* classe d'équivalence montre que la cardinalité de U est la somme des cardinalités de ses classes d'équivalences *différentes*. En formule

$$|U| = \sum_{C \in (U/\sim)} |C|.$$

Ou si $(U/\sim) = \{C_1, C_2, \ldots, C_m\}$ alors $U = C_1 \cup C_2 \cup \ldots C_m$ et $|U| = |C_1| + |C_2| + \ldots |C_m|$.

9.5. **Fonctions.** Nous obtenons une fonction surjective :

$$\mathrm{C}\ell : U \to U/\sim$$

ou $u \in U$ est envoyé à sa classe d'équivalence $\mathrm{C}\ell(u) \in U/\sim$. Cette fonction est importante, car cette fonction permet de "transport d'information" d'une côté à l'autre, comme un pont entre les deux ensembles.

Soit $C \in (U/\sim)$, alors son préimage par la fonction $\mathrm{C}\ell$ est le sous-ensemble $C \subseteq U$, c.-à-d., $\mathrm{C}\ell^{-1}(C) = C$.

Une fonction $f : U \to V$ telle que $f(u_1) = f(u_2)$ si $u_1 \sim u_2$ définit une fonction

$$\overline{f} : (U/\sim) \to V$$

par

$$\overline{f}(\mathrm{C}\ell(u)) := f(u).$$

Cette définition ne dépend pas du choix de u, car si $\mathrm{C}\ell(u_1) = \mathrm{C}\ell(u_2)$ alors $u_1 \sim u_2$ et donc $f(u_1) = f(u_2)$, par l'hypothèse dur f.

Sans cette hypothèse $\overline{f}(\mathrm{C}\ell(u)) := f(u)$ ne serait pas nécessairement *bien définie* : car si $\mathrm{C}\ell(u) = \mathrm{C}\ell(u')$ on veut $\overline{f}(\mathrm{C}\ell(u)) = \overline{f}(\mathrm{C}\ell(u'))$ et donc aussi que $f(u) = f(u')$: la condition est nécessaire et suffisante pour que c'est une définition d'une fonction !

9.6. **Exemples de relations d'équivalence.**

9.6.1. *Via une partition.* Supposons que nous avons une *partition* de U en sous-ensembles non-vide. C.-à-d. il existe une collection de sous-ensembles non-vides A_i, paramétrisée par un ensemble I, telle que $A_i \cap A_j = \emptyset$ si $i \neq j$. On obtient une relation d'équivalence : $u_1 \sim u_2$ s'il existe un $i \in I$ tel que $u_1 \in A_i$ et $u_2 \in A_i$.

Les classes d'équivalence sont exactement les sous-ensembles A_i pour $i \in I$.

9.6.2. *Via une fonction.* Si $f : U \to V$ est une fonction, on obtient une relation d'équivalence sur U si on *définit* : $u_1 \sim u_2$ si $f(u_1) = f(u_2)$.

Dans ce cas $\mathrm{C}\ell(u) = \{u' \in U |\ f(u') = f(u)\}$. La fonction de $U/\sim$ dans $\mathrm{Im}(f)$ qui associe à $\mathrm{C}\ell(u)$ la valeur $f(u)$ est une bijection.

9.6.3. *Relations d'équivalence $\equiv_m$ sur $\mathbb{Z}$.* Chaque nombre naturel $m > 0$ donne la relation d'équivalence *modulo* m , noté $\equiv_m$, déjà discuté :

On écrit que $n_1 \equiv_m n_2$ si $m|(n_1 - n_2)$. Autre notation $n_1 \equiv n_2 \bmod m$.

La classe de n est notée $\mathrm{C}\ell_m(n)$ ou $\mathrm{C}\ell(n)$ si m est fixé dans la discussion.

L'ensemble des classes $\mathbb{Z}/\equiv_m$ est noté $\mathbb{Z}/m\mathbb{Z}$.

Donc on peut considérer $\mathrm{C}\ell_m(n)$ comme un élément de $\mathbb{Z}/m\mathbb{Z}$ ou comme un certain sous-ensemble de $\mathbb{Z}$. Mais on ne peut pas le considérer comme un nombre entier.

On définit ensuite $\mathrm{C}\ell_m(n_1)+\mathrm{C}\ell_m(n_2) := \mathrm{C}\ell_m(n_1+n_2)$ et $\mathrm{C}\ell_m(n_1)\cdot\mathrm{C}\ell_m(n_2) := \mathrm{C}\ell_m(n_1\cdot n_2)$.

9.6.4. *Les fractions.* Les fractions, éléments de $\mathbb{Q}$, sont définies en utilisant une relation d'équivalence.

Sur l'ensemble $U := \{(n,d) \in \mathbb{Z}\times\mathbb{Z}|\ d \neq 0\}$ nous définissons

$$(n,d) \sim (n',d') \text{ si et seulement si } \ nd' = n'd.$$

Lemme 9.2. *$\sim$ est une relation d'équivalence sur U.*

Démonstration. Soient (n_1,d_1), (n_2,d_2) et (n_3,d_3) trois éléments de U, c.-à-d., n_1,n_2,n_3 trois entiers, et d_1,d_2,d_3 trois non-zéro entiers.

Il faut vérifier trois choses.

(i) $(n_1,d_1) \sim (n_1,d_1)$; c'est le cas car $d_1n_1 = d_1n_1$.

(ii) si $(n_1,d_1) \sim (n_2,d_2)$ alors $(n_2,d_2) \sim (n_1,d_1)$; c'est le cas car $n_1d_2 = n_2d_1$ implique que $n_2d_1 = n_1d_2$.

(iii) si $(n_1,d_1) \sim (n_2,d_2)$ et $(n_2,d_2) \sim (n_3,d_3)$ alors $(n_1,d_1) \sim (n_3,d_3)$. Pour montrer ça, supposons que l'hypothèse est vraie, c.-à-d. $n_1d_2 = n_2d_1$ et $n_2d_3 = n_3d_2$. Alors aussi $n_1d_2d_3 = n_2d_1d_3$ et $n_2d_3d_1 = n_3d_2d_1$ et $n_1d_2d_3 = n_3d_2d_1$. Donc $d_2(n_1d_3 - n_3d_1) = 0$. Ici, nous avons seulement utilisé les propriétés élémentaires de $\mathbb{Z}$, comme la commutativité et l'associativité pour la multiplication et la distributivité.

Nous avons aussi la propriété suivante pour deux entiers r et s : si $rs = 0$ et $r \neq 0$ alors nécessairement $s = 0$.

Appliquons cette propriété. Par hypothèse $d_2 \neq 0$ et $d_2(n_1d_3 - n_3d_1) = 0$. Donc nécessairement $(n_1d_3 - n_3d_1) = 0$, ou $n_1d_3 = n_3d_1$, ou $(n_1,d_1) \sim (n_3,d_3)$.

Alors en effet, $\sim$ est une relation d'équivalence sur U. □

Nous connaissons déjà depuis longtemps ses classes d'équivalence.

Définition 9.2. *(i) Pour $(n,d) \in U$ (donc n,d sont deux entiers, dont $d \neq 0$) nous allons écrire*

$$\frac{n}{d} := \mathrm{C}\ell(n,d)$$

pour la classe d'équivalence de $(n,d) \in U$. Nous allons appeler $\frac{n}{d}$ une fraction.

(i) Nous définissons

$$\mathbb{Q} := U/\sim,$$

l'ensemble des fractions.

En particulier $\frac{n_1}{d_1} = \frac{n_2}{d_2}$ (comme fractions) si et seulement si (par définition) $n_1 d_2 = n_2 d_1$. Par exemple $\frac{2}{5} = \frac{6}{15}$, car $2 \cdot 15 = 6 \cdot 5 = 30$.

Nous *définissons* l'addition et la multiplication

$$\frac{n_1}{d_1} + \frac{n_2}{d_2} := \frac{n_1 d_2 + n_2 d_1}{d_1 d_2}$$
$$\frac{n_1}{d_1} \cdot \frac{n_2}{d_2} = \frac{n_1 n_2}{d_1 d_2}$$

L'application de $\mathbb{Z}$ dans $\mathbb{Q}$ qui associe à n la fraction $\frac{n}{1}$ est injective. Souvent on ne fait pas distinction entre n et $\frac{n}{1}$ (malgré que l'un est un entier et l'autre une fraction).

Donc à partir des entiers, nous avons construit les fractions.

À partir de certaines suites d'éléments de $\mathbb{Q}$ et une relation d'équivalence on *construit* les nombres réels comme classe d'équivalence et $\mathbb{R}$ comme l'ensemble des classes d'équivalence. Mais c'est trop tôt de donner les détails ici.

Exemple 9.1. Est-ce que $f : \mathbb{Q} \to \mathbb{Z}$ avec $f(\frac{n}{m}) = n + m$ est une fonction ? Non. Pourquoi pas ?

9.6.5. *Un exemple avec des ensembles.* L'exemple suivant est en principe facile, mais est difficile si on ne sait pas encore de faire la distinction entre sous-ensemble et élément.

Soit E un ensemble fini, disons $|E| = n$. Considérons maintenant $U = P(E)$, l'ensemble des sous-ensembles de E. *Donc un élément de U est un sous-ensemble de E.* On va classifier les sous-ensemble *selon la taille.*

Soient A_1 et A_2 deux éléments de $U = P(E)$, c.-à-d., deux sous-ensembles de E. Nous disons que A_1 et A_2 sont dans la même classe, et on écrit $A_1 \sim A_2$, si $|A_1| = |A_2|$, alors si les deux sous-ensembles ont la même taille.

On a trivialement

- $A_1 \sim A_1$,
- si $A_1 \sim A_2$ alors $A_2 \sim A_1$,
- si $A_1 \sim A_2$ et $A_2 \sim A_3$ alors $A_1 \sim A_3$.

Une *classe d'équivalence* est par définition la collection de tous les sous-ensembles de même taille. L'ensemble de tous les sous-ensembles de E avec exactement i éléments est noté comme :

$$\binom{E}{i} := \{A \subset E |\ |A| = i\} \subset P(E),$$

On a ici $|U| = |P(E)| = 2^n$, mais la collection des classes d'équivalence (pour notre relation d'équivalence de ta latille) a donc seulement $n + 1$ éléments et est notée :

$$(U/\sim) = (P(E)/\sim)\ := \{\binom{E}{0}, \binom{E}{1}, \binom{E}{2}, \ldots, \binom{E}{n}\} \subseteq P(P(E))$$

Il y a une fonction surjective $\mathrm{C}\ell : P(E) \to (P(E)/\sim)$ telle que $\mathrm{C}\ell(A) = \binom{E}{i}$ si $A \in \binom{E}{i}$.

Remarque. Il faut comprendre les distinctions : Un élément A de $\binom{E}{i}$, ou $A \in \binom{E}{i}$, est par définition un sous-ensemble de E, $A \subset E$, tel que $|A| = i$.

Et $\binom{E}{i}$ est un élément de $(P(E)/\sim)$, mais $\binom{E}{i}$ est aussi un certain sous-ensemble de $P(E)$ et aussi une collection de sous-ensembles de E.

Chaque élément de $P(E)$ (=chaque sous-ensemble de E) est dans une *unique* classe d'équivalence. Et donc

$$P(E) = \bigcup_{i=0}^{n} \binom{E}{i}$$

est une *partition de* $P(E)$: c.-à-d. chaque $\binom{E}{i}$ est non-vide, et $\binom{E}{i}$ et $\binom{E}{j}$ sont disjoints si $i \neq j$.

En conséquence :

$$|P(E)| = \sum_{i=0}^{n} |\binom{E}{i}|$$

Par exemple, pour $E = \{a, b, c\}$.

$$\begin{aligned}
\binom{E}{0} &= \{\emptyset\}; \\
\binom{E}{1} &= \{\{a\}, \{b\}, \{c\}\}; \\
\binom{E}{2} &= \{\{b, c\}, \{a, c\}, \{a, b\}\}; \\
\binom{E}{3} &= \{E\}; \\
P(E) &= \binom{E}{0} \cup \binom{E}{1} \cup \binom{E}{2} \cup \binom{E}{3}; \\
P(E)/\sim &= \{\binom{E}{0}, \binom{E}{1}, \binom{E}{2}, \binom{E}{3}\}.
\end{aligned}$$

En particulier $a \in \{a, b\}$, $\{a, b\} \in \binom{E}{2}$, $\binom{E}{2} \in (P(E)/\sim)$. Mais aussi $\{a, b\} \subseteq E$, $\binom{E}{2} \subseteq P(E)$. Vous comprenez ? C'est important de comprendre les distinctions.

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA