André et Germaine REVUZ

LE COURS DE L'A.P.M.

I - Groupes, anneaux, corps

Les brochures de l'A.P.M.

6

Les brochures de l'A.P.M.

Collection de monographies utiles à l'enseignement des mathématiques.

1. **Le langage simple et précis des Mathématiques modernes,** par André REVUZ et Léonce LESIEUR (épuisé).

2. **Congruences paractiques de cycles,** par Paul ROBERT
(64 pages, 3 NF, franco 3,50 NF).

3. **Recherche d'une axiomatique commode pour le premier enseignement de la géométrie élémentaire,** par Gustave CHOQUET
(40 pages, 2 NF, franco 2,50 NF).

4. **Le calcul des probabilités et l'enseignement,** par A. HUISMAN, R. FORTET, E. MOURIER, A. FUCHS, D. DUGUE, G.-T. GUILBAUD, J. BOUZITAT, J. VILLE, F. GENUYS
(144 pages, 7 NF, franco 8 NF).

5. **L'enseignement de la mécanique,** par P. GERMAIN, R. MAZET, J. KAMPE, de FERIET
(40 pages, 2 NF, franco 2,50 NF).

7. **Etude commentée d'une méta-démonstration de Gödel,** par Jean BALIBAR
(40 pages, 2 NF, franco 2,50 NF).

En préparation.

- **Les Mathématiques « modernes » dans l'enseignement du second degré,** par André HUISMAN.

- **Le cours de l'A.P.M. II. Les espaces vectoriels,** par André et Germaine REVUZ.

Pour se procurer les brochures de l'A.P.M.,

Adresser commandes et virements postaux à l'Association des Professeurs de Mathématiques de l'Enseignement Public, C.C.P. Paris 5 708-21.
Préciser au dos du virement les brochures commandées.

Voir page 3 de la couverture les conditions d'adhésion à l'A.P.M.E.P.

M Leonhardt

André REVUZ
Professeur à la Faculté des Sciences de Poitiers

Germaine REVUZ
Maître-Assistant à la Faculté des Sciences de Poitiers

LE COURS DE L'A.P.M.

I

Groupes, anneaux, corps

Association des Professeurs
de Mathématiques de l'Enseignement Public
PARIS — 1962

Les brochures de l'A.P.M.

Collection de monographies utiles à l'enseignement des mathématiques.

1. **Le langage simple et précis des Mathématiques modernes,** par André REVUZ et Léonce LESIEUR (épuisé).

2. **Congruences paractiques de cycles,** par Paul ROBERT
(64 pages, 3 NF, franco 3,50 NF).

3. **Recherche d'une axiomatique commode pour le premier enseignement de la géométrie élémentaire,** par Gustave CHOQUET
(40 pages, 2 NF, franco 2,50 NF).

4. **Le calcul des probabilités et l'enseignement,** par A. HUISMAN, R. FORTET, E. MOURIER, A. FUCHS, D. DUGUE, G.-T. GUILBAUD, J. BOUZITAT, J. VILLE, F. GENUYS
(144 pages, 7 NF, franco 8 NF).

5. **L'enseignement de la mécanique,** par P. GERMAIN, R. MAZET, J. KAMPE, de FERIET
(40 pages, 2 NF, franco 2,50 NF).

7. **Etude commentée d'une méta-démonstration de Gödel,** par Jean BALIBAR
(40 pages, 2 NF, franco 2,50 NF).

En préparation.

- **Les Mathématiques « modernes » dans l'enseignement du second degré,** par André HUISMAN.

- **Le cours de l'A.P.M. II. Les espaces vectoriels,** par André et Germaine REVUZ.

Pour se procurer les brochures de l'A.P.M.,

Adresser commandes et virements postaux à l'Association des Professeurs de Mathématiques de l'Enseignement Public, C.C.P. Paris 5 708-21.
Préciser au dos du virement les brochures commandées.

Voir page 3 de la couverture les conditions d'adhésion à l'A.P.M.E.P.

André REVUZ
Professeur à la Faculté des Sciences de Poitiers

Germaine REVUZ
Maître-Assistant à la Faculté des Sciences de Poitiers

LE COURS DE L'A.P.M.

I

Groupes, anneaux, corps

Association des Professeurs
de Mathématiques de l'Enseignement Public
PARIS — 1962

« *Afin que, ... aux dépens d'autrui*
Sage, je m'enseignasse. »

REGNIER.

« *C'est assez désagréable... de ne pouvoir plus rien apprendre pour toute la vie ! Nos aïeux s'en tenaient aux enseignements qu'ils avaient reçus dans leur jeunesse : mais, nous, il nous faut recommencer tous les cinq ans, si nous ne voulons pas être complètement démodés.* »

GŒTHE (Les affinités électives).

Les brochures de l'A.P.M. mettent à la disposition des professeurs des textes utiles à l'enseignement.

Ou bien ces textes sont inédits, ou bien ils ont déjà paru, soit dans le Bulletin de l'A.P.M., soit ailleurs. Dans tous les cas, il a paru intéressant de regrouper des écrits sous une forme commode pour les maîtres qui auront à s'en servir.

Brochures parues :

1. Le langage simple et précis des mathématiques modernes, par A. REVUZ et L. LESIEUR, Professeurs à la Faculté des Sciences de Poitiers (avril 1960), **(épuisée).**
2. Congruences Paratactiques de cycles, par Paul ROBERT, Inspecteur général honoraire de l'Instruction Publique (avril 1960).
3. Recherche d'une axiomatique commode pour le premier enseignement de la géométrie élémentaire, par Gustave CHOQUET, Professeur à la Sorbonne (février 1961).
4. Le calcul des probabilités et l'enseignement, par A. HUISMAN, R. FORTET, E. MOURIER, A. FUCHS, D. DUGUE, G.-T. GUILBAUD, J. BOUZITAT, J. VILLE et F. GENUYS (novembre 1961).
5. L'enseignement de la mécanique, par P. GERMAIN, J. KAMPE DE FERIET et R. MAZET (novembre 1961).
6. Le cours de l'A.P.M. I. Groupes, anneaux, corps, par A. et G. REVUZ.
7. Etude commentée d'une méta-démonstration de Gödel, par J. BALIBAR.

Brochures en préparation :

- Les Mathématiques « modernes » dans l'enseignement du second degré, par A. HUISMAN.
- Le Cours de l'A.P.M. II. Les espaces vectoriels, par A. et G. REVUZ.

AVANT-PROPOS

Les pages qui suivent contiennent la matière d'un cours organisé à Paris par l'A.P.M.E.P. durant l'année scolaire 1960-1961, à raison d'une séance d'une heure et demie tous les quinze jours.

Conférencier, rédacteur du cours, correcteur des stencils (une polycopie du cours précédent et des solutions d'exercices était distribuée à chaque séance), organisateurs, auditeurs (leur nombre a dépassé deux cents) étaient tous bénévoles : ce qui prouve que les professeurs de Mathématiques n'hésitent pas à consacrer du temps et de la peine à approfondir leur culture, et témoigne de la vitalité de l'Association.

Ce cours ne prétend pas constituer un traité d'Algèbre parfaitement équilibré : les nécessités de l'horaire ont contraint à passer sous silence certaines questions importantes, comme l'étude élémentaire des groupes de substitutions, les anneaux euclidiens..., qui sont traitées dans un autre ouvrage d'initiation (Lentin et Rivaud), ou à ne les faire figurer que sous forme d'exercices (par exemple, la structure de corps de **Q**). *Il est à souhaiter d'autre part que de nombreux lecteurs aient envie d'aller au-delà de ce qui a été traité et désirent connaître, par exemple, la théorie des idéaux ou la théorie de Galois, qu'ils trouveront dans les ouvrages de Bourbaki, de Dubreil, de Van der Waerden...*

Soixante-six exercices ont été proposés. Leurs solutions sont groupées à la fin du volume. Ils sont de difficulté assez inégale, mais en général assez soutenue (il ne faut pas oublier qu'il s'agit d'un cours s'adressant à des professeurs !) : quelques applications immédiates, des exemples, des contre-exemples et un assez grand nombre de compléments importants à certains points du cours.

Des conférences d'initiation à ce qu'on appelle les Mathématiques modernes avaient été organisées les années précédentes en liaison avec la Société Mathématique de France. Le but du cours 1960-1961 était d'approfondir cette initiation par des exposés se déroulant plus lentement et n'hésitant pas à pénétrer dans le détail de certaines questions. Son ambition était de convaincre que les Mathématiques dites modernes ne s'opposent pas aux Mathématiques des âges précédents, mais sont essentiellement issues d'une prise de conscience *de ce qui restait trop souvent implicite. On retrouve toutes les Mathématiques classiques dans les Mathématiques modernes, mais on les retrouve sous un éclairage qui surprend parfois au premier abord, mais dont les avantages : cohérence, clarté des idées fondamentales, mise en ordre des théories, mise en évidence des raisons profondes des résultats, apparaissent bien vite.*

Dans cette mise en ordre, la notion de structure est l'outil essentiel. Pour parler brièvement, on peut dire qu'une théorie mathématique est l'étude d'une ou de plusieurs structures et de leurs homomorphismes, ou encore que l'esprit moderne pense en termes d'ensembles, de relations et d'applications, de structures et d'homomorphismes. C'est à acquérir cette mentalité que l'on a voulu aider le lecteur : pour ce faire, on n'a pas craint d'insister lourdement au départ, et de ne pas aller toujours droit au but. On remarquera, en particulier, que l'étude de l'homomorphisme des groupes est traitée lentement et non sans lourdeur, et que, quelques paragraphes plus loin, le théorème général sur la factorisation des homomorphismes de structures algébriques est exécuté en quelques lignes : c'est, assurément, cette dernière démonstration qui est la « bonne », mais on a pensé qu'il n'était pas mauvais d'avoir auparavant démonté dans le cas particulier des groupes le détail du mécanisme. De même, dans l'étude des nombres réels, on a cru devoir insister sur toutes les structures de **R** *et étudier en détail les deux méthodes fondamentales très différentes qui permettent de passer de* **Q** *à* **R**, *en ne cherchant pas l'élégance de l'exposé, mais la mise en lumière de la motivation de chacune des démarches effectuées.*

On assiste actuellement à une pénétration progressive de l'esprit moderne dans l'Enseignement du Second Degré. Un des buts de ce cours est d'y aider. On n'y trouvera cependant aucune allusion directe à l'Enseignement du Second Degré. L'objectif visé, et qui paraît bien raisonnablement le premier à atteindre, était de répandre chez les professeurs l'esprit des Mathématiques contemporaines. Un second objectif sera de déterminer comment cet esprit peut pleinement se développer dans l'Enseignement élémentaire, dont une des tâches est certainement de faire prendre conscience, dans les démarches intellectuelles les plus familières à l'humanité du XX^{e} *siècle, des structures mathématiques qui en sont le fondement. Il faut souhaiter que de futures « brochures de l'A.P.M. » soient prochainement consacrées à cette étude, et qu'elles naissent, comme celle-ci, et plus encore que celle-ci, d'un travail collectif au sein de l'Association.*

André Revuz.

TABLE DES MATIÈRES

CHAPITRE PREMIER. — ENSEMBLES. RELATIONS.

CHAP. 2. — GROUPES.

Errata

Page 15, lignes 5 et 8, *lire :* **R** *au lieu de :* R.
ligne 6, *lire :* **N** *au lieu de :* N.

Page 16, ligne 4, *lire :* étant donnée *au lieu de :* étant donné.
ligne 18, *lire :* **R** *au lieu de :* R.

Page 19, n° 10, ligne 5, *lire :* **N** *au lieu de :* N.

Page 23, ligne 7, *lire :* $\forall (a, b, c) \in E^3 \quad aRb$ et $bRc \Rightarrow aRc$
au lieu de : $\forall (a, b, c) \in E^2 \quad aRb \Rightarrow$ non bRa.
ligne 4 du bas, *lire :* **R** *au lieu de :* R.

Page 29, dernière ligne de la note, *supprimer la virgule après* partout.

Page 31, 2. ligne 7, *ajouter une virgule entre* $a\,x = b$ *et* $x = a^{-1}b$.

Page 34, ligne 16, *lire :* ci-dessus *au lieu de :* ci-contre.

Page 35, exemples, lignes 1 et 6, *lire :* **R** *au lieu de :* R.

Page 39, ligne 4 du bas, *lire :* $\dot{x}$ *au lieu de :* x.

CHAPITRE I

ENSEMBLES - RELATIONS

§ 1. NOTION D'ENSEMBLE. ALGEBRE DES ENSEMBLES

1. Les ensembles.

Les Mathématiques prenant leur départ dans la notion d'ensemble, il s'agit d'une notion première donc exempte de définition. En fait, cette notion s'est élaborée par abstraction de celle de *collection,* de collections finies d'abord, puis de collections infinies.

Exemples : l'ensemble des droites d'un plan ;
l'ensemble N des entiers naturels.

La considération de collections infinies repose sur une axiomatique précise (il y en a d'ailleurs plusieurs possibles). Ces axiomatiques aboutissent à ne pas considérer comme ensembles certaines collections trop vastes, considération qui conduirait à des paradoxes (*). Nous ne nous attarderons pas ici sur cette question et nous admettrons qu'un ensemble est déterminé dès l'instant qu'on sait décider de l'appartenance d'un élément à cet ensemble.

2. Appartenance.

Un élément a étant donné, il faut pouvoir décider par oui ou par non s'il appartient à l'ensemble.

Dans le premier cas on écrira :

$$a \in E.$$

Dans le deuxième :

$$a \notin E.$$

Exemple :

$$3 \in N \qquad 2/7 \notin N.$$

(*) Parmi les différentes positions que l'on peut adopter à ce point de vue, citons la suivante : accepter comme ensembles, l'ensemble N des entiers naturels et tous ceux que l'on peut en déduire : 1) comme partie d'un ensemble déjà considéré ; 2) comme ensemble des parties d'un ensemble déjà considéré ; 3) comme produits cartésiens d'ensembles déjà considérés. Cette position suffit, pour les besoins des mathématiques, jusqu'à un niveau assez élevé et a l'avantage de n'introduire que des ensembles que l'on peut construire de manière assez « naturelle » à partir d'un ensemble lui-même très « naturel ».

Remarquons que dans des questions non mathématiques on peut se trouver dans une situation différente ; il peut y avoir une zone indécise où on ne sait pas répondre par oui ou par non (dans les classifications d'histoire naturelle, par exemple). Nous supposerons toujours en Mathématiques qu'il n'en est pas ainsi. Un ensemble est souvent défini comme celui des éléments x qui possèdent une propriété P. On notera un tel ensemble :

$$\{ x ; P \}$$

Exemples : le cercle du plan P, de centre O, de rayon R, s'écrira :

$$\{ M ; M \in P, OM = R \} ;$$

l'ensemble des nombres impairs :

$$\{ x ; x \in N, x \equiv 1 \pmod 2 \} .$$

Remarque : Il est prudent, dans l'enseignement élémentaire, d'exclure *à priori* toute relation de la forme $a \in a$. On peut considérer comme intuitif qu'elle est dépourvue de sens et qu'il est absurde de considérer un être qui puisse être à la fois un ensemble et un élément de cet ensemble. Il faut noter cependant que les théories formelles n'imposent en général pas explicitement cette condition, mais sont agencées de telle sorte que tout être qui satisferait à $a \in a$ est exclu de la théorie. Imposer la condition dès le départ a l'avantage de couper court à toutes les discussions prématurées que ne manqueraient de faire naître certains élèves en considérant des monstres tels que « l'ensemble de tous les ensembles ».

3. Inclusion et égalité.

Si 2 ensembles A et B sont tels que :

$$a \in A \Rightarrow a \in B$$

(le signe $\Rightarrow$ se lisant « implique », comme le signe $\Longleftrightarrow$ se lira « équivaut à »), on dit que A est *inclus* dans B et on écrit :

$$A \subset B \quad \text{ou} \quad B \supset A$$

La relation d'inclusion est transitive :

$$A \subset B \text{ et } B \subset C \Rightarrow A \subset C.$$

Si $A \subset B$ et $B \subset A$, les ensembles sont constitués des mêmes éléments ; on dit qu'ils sont *égaux* et on écrit :

$$A = B.$$

On emploie le terme d'*inclusion stricte* pour caractériser le cas :

$$A \subset B \qquad A \neq B.$$

Quand A est inclus dans B, on dit aussi que :

A est une *partie* de B
ou A est un *sous-ensemble* de B.

Il importe de ne pas confondre l'appartenance d'un élément à un ensemble et l'inclusion d'un ensemble dans un autre,

$$a \in A \text{ avec } B \subset A.$$

4. Ensemble des parties d'un ensemble.

On appelle ainsi l'ensemble dont les éléments sont les sous-ensembles d'un ensemble E. On le note par

$$\mathcal{P}(E).$$

Un sous-ensemble de $\mathcal{P}(E)$ est une famille de sous-ensembles de E. Il est commode de codifier les notations :

minuscules latines pour les éléments de E : $a \in E$,
majuscules latines pour les parties de E : $A \subset E$ ou $A \in \mathcal{P}(E)$,

majuscules gothiques (ou rondes) pour les familles de parties :

$$\mathcal{A} \subset \mathcal{P}(E), \text{ c'est-à-dire } \mathcal{A} \in \mathcal{P}\mathcal{P}(E).$$

Une partie de E peut ne contenir que l'élément a ; on la note alors par :

$$\{ a \},$$

qu'il faut distinguer de a. $a \in \{ a \}$ a un sens, $a \in a$ n'en a pas (cf. I. 1, 2).

Parmi les éléments de $\mathcal{P}(E)$, il ne faut pas oublier l'ensemble E lui-même et l'ensemble vide qui ne contient aucun élément et est noté : $\emptyset$.

Exercice 1. — Si E a n éléments, $\mathcal{P}(E)$ a 2^n éléments.

5. Complémentaire d'un ensemble.

Soit un ensemble E et $A \in \mathcal{P}(E)$. L'ensemble des éléments x de E qui n'appartiennent pas à A est appelé le complémentaire de A par rapport à E que l'on note :

$$\complement_E A$$

ou, si aucune confusion n'est à craindre, $\complement A$.

Cette définition s'écrit : $\complement A = \{ x ; x \in E, x \notin A \}$.

Propriétés :

$$\complement\complement A = A \qquad \complement E = \emptyset.$$

6. Quantificateurs logiques.

Ce sont les 2 signes :

$\forall$ qui se lit « pour tout »,
$\exists$ qui se lit « il existe » pris dans le sens de « il existe au moins un ».

Si $x \in E \Rightarrow x,\ P,$
c'est-à-dire si tout x possède la propriété P, on écrira :

$$\forall x \in E,\ P,$$

et s'il existe parmi les éléments de E au moins un élément qui possède P, c'est-à-dire si

$$\{ x ; x \in E, x,\ P \} \neq \emptyset,$$

on écrira plus brièvement :

$$\exists x \in E,\ P.$$

Lien entre les deux quantificateurs. Soit l'ensemble E tel que :

$$\forall x \in E,\ P.$$

La négation de cette propriété, c'est que l'ensemble des x de E qui possèdent la propriété contradictoire, ensemble qui est le complémentaire de $\{ x ; x \in E\ x\ P \}$, n'est pas vide, ce qui peut s'écrire :

$$\exists x \in E,\ x \text{ non P}.$$

D'où l'énoncé :

$$\text{non } (\forall x \in \text{E}, \quad \text{P}) \Longleftrightarrow \exists x \in \text{E}, \quad \text{non P}.$$

De même :

$$\text{non } (\exists x \in \text{E}, \text{P}) \Longleftrightarrow \forall x \in \text{E}, \quad \text{non P}.$$

L'introduction des quantificateurs $\forall$ et $\exists$ permet un véritable automatisme pour passer d'une proposition à sa contradictoire. Lorsqu'il s'agit d'une proposition simple : « Toutes les Françaises sont blondes » et de sa négation : « Il existe une Française non blonde », le symbolisme peut sembler superflu. Il n'en est plus de même pour la proposition : « La fonction réelle f de la variable réelle x est continue pour x_0 » qui s'écrit symboliquement :

$$\forall \varepsilon > o \ \exists \eta > o \ \forall x \in]\, x_o - \eta, x_o + \eta [: |f(x) - f(x_o)| < \varepsilon,$$

dont la négation s'écrit automatiquement :

$$\exists \varepsilon > o \ \forall \eta > o \ \exists x \in]\, x_o - \eta, x_o + \eta \,[: |f(x) - f(x_o)| \geqslant \varepsilon.$$

Un autre exemple de l'utilité des quantificateurs nous est fourni par l'expérience faite par un collègue allemand qui présenta à ses étudiants (niveau propédeutique) le raisonnement suivant : Aucune opération ne peut être non commutative ; en effet, ceci signifierait $a + b \neq b + a$. Faisons $a = b$; on arrive à $a + a \neq a + a$, ce qui est impossible. 22 étudiants sur 72 seulement virent que la faute de raisonnement résidait dans le fait que la négation de

$\forall\,(a, b) \quad a + b = b + a$ (commutativité de l'opération $+$)

était

$\exists\,(a, b) \quad a + b \neq b + a$

et non pas

$\forall\,(a, b) \quad a + b \neq b + a$, comme le raisonnement l'admettait implicitement.

Opérations sur les parties d'un ensemble (*)

7. Intersection.

L'intersection de 2 ensembles A et B, partie d'un même ensemble E, notée par

$$\text{A} \cap \text{B}$$

est l'ensemble formé par les éléments qui appartiennent à la fois à A et à B :

$$x \in \text{A} \cap \text{B} \Longleftrightarrow x \in \text{A}, \ x \in \text{B}.$$

Propriétés. L'intersection est une opération *commutative* et *associative.*

$$\text{A} \cap \text{B} = \text{B} \cap \text{A}$$
$$(\text{A} \cap \text{B}) \cap \text{C} = \text{A} \cap (\text{B} \cap \text{C})$$

On notera ce dernier ensemble $\text{A} \cap \text{B} \cap \text{C}$.

(*) Les opérations que nous définissons dans ce paragraphe peuvent être effectuées sur deux ensembles quelconques, mais dans la pratique mathématique courante, elles ne sont considérées que pour les *parties d'un même ensemble ;* nous nous en tiendrons, ici, à ce point de vue.

Deux ensembles dont l'intersection est vide,

$$\text{A} \cap \text{B} = \emptyset$$

sont dits *disjoints.*

8. Réunion.

La réunion de 2 ensembles A et B parties d'un même ensemble, notée par

$$\text{A} \cup \text{B}$$

est l'ensemble des éléments qui appartiennent à l'un *ou* l'autre des deux ensembles (ou n'étant pas disjonctif), c'est-à-dire à au moins un des 2 ensembles.

$$x \in \text{A} \cup \text{B} \Longleftrightarrow x \in \text{A} \text{ ou } x \in \text{B}$$

ce que l'on peut encore énoncer :

$$x \in \text{A} \cup \text{B} \Longleftrightarrow (x \notin \text{A} \Rightarrow x \in \text{B})$$

Propriétés. La réunion est une opération *commutative* et *associative :*

$$\text{A} \cup \text{B} = \text{B} \cup \text{A}$$
$$(\text{A} \cup \text{B}) \cup \text{C} = \text{A} \cup (\text{B} \cup \text{C}) = \text{A} \cup \text{B} \cup \text{C}$$

La réunion et l'intersection sont *distributives* l'une par rapport à l'autre :

$$(\text{A} \cup \text{B}) \cap \text{C} = (\text{A} \cap \text{C}) \cup (\text{B} \cap \text{C})$$
$$(\text{A} \cap \text{B}) \cup \text{C} = (\text{A} \cup \text{C}) \cap (\text{B} \cup \text{C})$$

Le soin des démonstrations de ces diverses formules est laissé au lecteur. Le recours à un schéma peut aider l'intuition.

Relation avec le complémentaire. On voit tout de suite que

$$\complement(\text{A} \cup \text{B}) = \complement\text{A} \cap \complement\text{B}$$
$$\complement(\text{A} \cap \text{B}) = \complement\text{A} \cup \complement\text{B}$$

Il en résulte qu'à toute formule comportant les signes de réunion, d'intersection et de complémentaire, et ne comportant qu'eux, correspond une formule dite *duale* de la première obtenue par échange des signes de réunion et d'intersection et remplacement des ensembles par leurs complémentaires. C'est ainsi que la première des formules de distributivité écrite ci-dessus donne :

$$(\complement\text{A} \cap \complement\text{B}) \cup \complement\text{C} = (\complement\text{A} \cup \complement\text{C}) \cap (\complement\text{B} \cup \complement\text{C})$$

Mais A, B, C, étant 3 éléments arbitraires de $\mathcal{P}(\text{E})$, leurs complémentaires sont aussi arbitraires et la formule obtenue en négligeant les signes complémentaires est encore vraie. C'est la deuxième, duale de la première. Elle a donc été obtenue, à partir de la première, par simple échange des signes de réunion et d'intersection. Le fait est général : quand une identité ne comporte que des signes de réunion et d'intersection, on obtient sa duale par échange de ces signes.

9. Différence symétrique

notée par $\text{A} \vartriangle \text{B}$.

On pose :

$$\text{A} \vartriangle \text{B} = \{x \,;\, x \in \text{A}, x \notin \text{B} \text{ ou } x \notin \text{A}, x \in \text{B}\}$$

10. Différence.

On pose :

$$A - B = \{x\,;\, x \in A, x \notin B\} = A \cap \complement B$$

Exercice 2. — Montrer que :

$$A \Delta B = A \cup B - A \cap B = (A - B) \cup (B - A)$$

Exercice 3. — Montrer que la différence symétrique est une opération associative ; caractériser les éléments de $A \Delta B \Delta C$. Montrer (en anticipant sur la suite des cours) que la différence symétrique donne une structure de groupe commutatif à l'ensemble des parties d'un ensemble ; quel en est l'élément neutre ?

Exercice 4. — Soit $\mathcal{F} \subset \mathcal{P}(E)$ une famille de parties qui satisfait aux conditions suivantes :

$$A, B \in \mathcal{F} \Rightarrow A \cup B \in \mathcal{F}, A - B \in \mathcal{F}$$

a) Démontrer que la propriété de définition équivaut à la suivante :

$$A, B \in \mathcal{F} \Rightarrow A \Delta B \in \mathcal{F}, A \cap B \in \mathcal{F}$$

Montrer (en anticipant encore sur la suite) que $\mathcal{F}$ a pour ces deux dernières opérations une structure d'anneau commutatif.

b) Montrer que, l'ensemble E étant une droite, la famille dont chaque élément est une réunion finie de semi-segments ouverts à droite ($a \leqslant x < b$) est une famille $\mathcal{F}$. (On observera d'abord que toute réunion finie de semi-segments est une réunion finie de semi-segments 2 à 2 disjoints).

11. Produit cartésien d'ensembles.

Etant donnés 2 ensembles E et F, on appelle produit cartésien noté

$$E \times F$$

l'ensemble des couples d'un élément de E et d'un élément de F :

$$E \times F = \{(x, y)\,;\, x \in E, y \in F\}$$

Exemple : Le plan est le produit cartésien d'une droite par une droite, ou encore :

$$\mathbf{R} \times \mathbf{R} = \mathbf{R}^2$$

R représentant l'ensemble des réels.

On posera de même :

$$E_1 \times E_2 \times E_3 = \{(x_1, x_2, x_3)\,;\, x_1 \in E_1, x_2 \in E_2, x_3 \in E_3\}$$

On dit que (x_1, x_2, x_3) *décrit* le produit lorsque x_1 décrit E_1, x_2, décrit E_2...

§ 2. RELATIONS ET APPLICATIONS

1. Relation binaire.

Etant donnés 2 ensembles E et F (qui peuvent être identiques), on dit qu'une relation est définie entre les éléments de E et ceux de F si, de tout couple (x, y), $x \in E$, $y \in F$, on sait s'il vérifie ou non la relation.

La donnée d'une relation est alors celle d'un sous-ensemble du produit cartésien $E \times F$. Ce sous-ensemble est appelé *graphe* de la relation.

Soit R une relation. On indiquera que le couple (x, y) la vérifie en écrivant :

$$x\mathrm{R}y \qquad \text{ou bien } (x, y) \in \mathcal{R}$$

$\mathcal{R} \in \mathcal{P}(E \times F)$ étant le graphe de la relation.

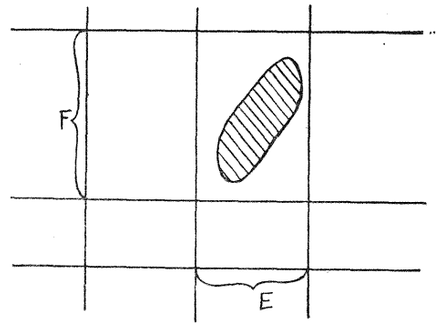


FIG. 1

E et F étant des segments de la droite réelle $\mathbf{R}$, le graphe est un sous-ensemble du rectangle construit sur E et F.

Exercice 5. — Si E = N, F = N, tracer le graphe de la relation : x et y ont même parité.

Si E et F ne sont pas des segments de $\mathbf{R}$, on peut encore utiliser le dessin ci-dessus, non pas comme donnant le véritable graphe, mais comme un schéma.

2. Relation ternaire.

Elle sera définie de même par la donnée d'une partie de

$$E_1 \times E_2 \times E_3$$

3. Fonctions et applications.

Supposons donnée une relation R entre $x \in E$ et $y \in F$. Nous posons la question de savoir si, x étant donné, il existe y tel que $x\mathrm{R}y$.

1er cas. — Pour tout $x \in E$, il existe *au plus* un y tel que

$$x\mathrm{R}y$$

On dira qu'une telle relation est *une fonction définie dans* E *et à valeurs dans* F.

On appellera *ensemble de définition* de la fonction l'ensemble :

$$\{x\,;\, x \in E \quad \exists y\,;\, x\mathrm{R}y\}$$

c'est-à-dire l'ensemble des x pour lesquels il existe exactement un y.

2e cas (plus restrictif). — Pour tout $x \in E$, il existe exactement un y tel que xRy. La relation est alors appelée *application* de E dans F ou encore application définie sur E et à valeurs dans F. Observons tout de suite que, étant donnée une fonction, quand on a déterminé son ensemble de définition, on se trouve en présence d'une application définie sur cet ensemble (*).

Notations. On désignera une application de E dans F par une seule lettre f et on écrira schématiquement :

$$f : E \longrightarrow F \text{ ou } E \xrightarrow{f} F$$

On pourra aussi dans certains cas se contenter de la flèche et écrire :

$$E \longrightarrow F$$

Une autre possibilité, si E et F ont déjà été nettement indiqués, est d'écrire :

$$x \longrightarrow f(x)$$

où x désigne un élément arbitraire de E et $f(x)$ l'élément de F image de x par l'application f.

Cette dernière notation semble assez indiquée pour les fonctions usuelles telles que, x décrivant $\mathbb{R}$,

$$x \longrightarrow 2x^2 + x + 3$$

On s'abstiendra en tout cas de la très fâcheuse appellation habituelle : « la fonction $f(x)$ », qui crée une regrettable confusion entre l'application f qui est un élément de $\mathcal{P}(E \times F)$, et $f(x)$ qui est un élément de F.

Nous désignerons par $\mathcal{F}(E \times F)$ l'ensemble des applications de E dans F. $\mathcal{F}(E \times F)$ est une partie de $\mathcal{P}(E \times F)$.

4. Classification des applications.

1) Nous nous posons maintenant la question : la proposition suivante est-elle exacte ?

$$\forall y \in F \quad \exists x \quad y = f(x) \qquad (1).$$

Autrement dit, tout élément de F est-il obtenu par l'application comme image d'éléments de E ?

Si (1) est vraie, on dit que l'application f est une application de E *sur* F, ou qu'elle est *surjective*, ou encore que c'est une *surjection*.

2) Soient maintenant les éléments de y qui sont obtenus par f, donc tels qu'il existe au moins un x tel que $y = f(x)$. Il peut y en avoir un seulement, ce qui revient à dire :

$$\forall x \in E \quad \forall u \in E \quad x \neq u \Rightarrow f(x) \neq f(u)$$

Dans ce cas, on dit que l'application est *injective* ou que c'est une *injection*.

(*) La distinction que nous introduisons ici entre fonction et application n'est pas faite par la plupart des auteurs, qui considèrent les deux termes comme rigoureusement synonymes. Elle a l'avantage de s'adapter au cas, fréquent dans l'enseignement élémentaire, où l'expression du nombre réel $f(x)$ est donnée avant que l'on ait déterminé pour quelles valeurs réelles de x, $f(x)$ était calculable : pratique qui n'est sans doute pas très recommandable, mais qu'il n'est pas toujours facile d'éviter. Il ne semble en tout cas pas mauvais, lorsque l'on dispose de deux synonymes, de spécialiser le sens de l'un d'entre eux pour accroître les ressources du langage.

3) Si maintenant une application jouit des 2 propriétés précédentes à la fois, on dit qu'elle est *bijective* ou que c'est une *bijection* (ou encore une correspondance biunivoque).

5. Restriction.

Soit :

$$E \xrightarrow{f} F$$

une application de E dans F, et soit $A \subset E$. L'application qui fait correspondre aux éléments x de A leur image dans F par f :

$$x \in A \longrightarrow f(x) \in F$$

est dite restriction de f à A.

6. Extension.

Soit :

$$A \xrightarrow{f} F$$

et soit $E \supset A$; une application g de E dans F, dont la restriction à A est f, est dite une extension de f à E. Une application n'a qu'une restriction à un ensemble donné, mais elle a, en général, une infinité d'extensions à un ensemble donné.

Exercice 6. — Déterminer dans quels cas une application de A dans F n'a qu'un nombre fini d'extensions à un vrai sur-ensemble de A.

7. Composition des applications.

Soient :

$$E \xrightarrow{f} F \xrightarrow{g} G.$$

Il existe une application de E dans G :

$$x \in E \longrightarrow g[f(x)] \in G.$$

Cette application est dite *composée des 2 applications* et est notée :

$$g \circ f.$$

D'après sa définition même, cette opération est associative :

$$h \circ (g \circ f) = (h \circ g) \circ f$$

Exercice 7. —

1) Soient f et g, deux applications quelconques, et i, une application injective. Montrer que :

$$i \circ f = i \circ g \Rightarrow f = g$$

Enoncer et démontrer une réciproque.

2) Soit maintenant s, une surjection. Montrer que :

$$f \circ s = g \circ s \Rightarrow f = g$$

Enoncer et démontrer une réciproque.

8. Image par une application f d'une partie A de E.

On appelle ainsi l'ensemble :

$$f(A) = \{ f(x) \; ; \; x \in A \}$$

A appartenant à $\mathcal{P}(E)$, $f(A)$ appartient à $\mathcal{P}(F)$.

On a donc défini une nouvelle application :

$$\mathcal{P}(E) \longrightarrow \mathcal{P}(F)$$

que l'on peut considérer comme une extension à $\mathcal{P}(E)$ de l'application précédemment définie sur les seuls éléments de $\mathcal{P}(E)$ réduits à un seul élément. On convient de garder la même notation f pour cette nouvelle application.

Exercice 8. — Comparer :

$$f(A \cup B) \text{ et } f(A) \cup f(B)$$
$$f(A \cap B) \text{ et } f(A) \cap f(B)$$
$$f(\complement_E A) \text{ et } \complement_F f(A)$$

9. Inversion d'une application.

Une application

$$E \xrightarrow{f} F$$

étant donnée, revenons à la question : Pour $y \in F$, existe-t-il un x tel que $y = f(x)$?

D'abord, si f n'est pas surjective, on ne peut affirmer l'existence d'un tel x.

Ensuite, si f est surjective sans être injective, à un y peut correspondre plusieurs x.

C'est donc seulement dans le cas d'une application bijective qu'à tout y correspond un x et un seul et qu'*il existe une application inverse* g,

$$F \xrightarrow{g} E$$

définie par :

$$x = g(y) \text{ si } y = f(x).$$

Notons que :

$$\forall x \in E \qquad g \circ f(x) = x,$$
$$\forall y \in F \qquad f \circ g(y) = y.$$

L'application $g \circ f = I_E$ sera dite *application identique* de E sur lui-même. De même, $f \circ g = I_F$.

Exercice 9. — Montrer que, réciproquement, l'existence d'une application g qui satisfait à

$$g \circ f = I_E \qquad f \circ g = I_F$$

est une condition suffisante pour que f soit bijective. Que peut-on dire de f si une seule des deux égalités précédentes est vérifiée ?

Cas où f n'est pas bijective. Nous pouvons encore considérer l'ensemble :

$$\{x \,;\, y = f(x)\}$$

qui dans le cas d'une bijection ne contenait qu'un élément. A un élément y de F, nous faisons donc correspondre une partie de E. Il est alors plus intéressant de considérer plus symétriquement une correspondance entre $\mathcal{P}(F)$ et $\mathcal{P}(E)$.

Etant donné $A \in \mathcal{P}(F)$, nous considérons l'ensemble :

$$\{x \,;\, f(x) \in A\}$$

que l'on appelle image réciproque de A par f. On définit ainsi une application de $\mathcal{P}(F)$ dans $\mathcal{P}(E)$ que l'on note $\overset{-1}{f}$ et que l'on appelle *application réciproque de f.*

$$\mathcal{P}(F) \xrightarrow{\overset{-1}{f}} \mathcal{P}(E).$$

Exercice 10. — Comparer :

$$\overset{-1}{f}(A \cap B) \text{ et } \overset{-1}{f}(A) \cap \overset{-1}{f}(B)$$
$$\overset{-1}{f}(A \cup B) \text{ et } \overset{-1}{f}(A) \cup \overset{-1}{f}(B)$$
$$\overset{-1}{f}(\complement_F A) \quad \text{et} \quad \complement_E \overset{-1}{f}(A)$$

Exercice 11. — A étant une partie de E, comparer :

$$\overset{-1}{f} \circ f(A) \text{ et } A$$

Dans quel cas a-t-on l'égalité, quelle que soit $A \in \mathcal{P}(E)$?

A étant une partie de F, comparer :

$$f \circ \overset{-1}{f}(A) \text{ et } A$$

Dans quel cas a-t-on l'égalité, quelle que soit $A \in \mathcal{P}(F)$?

10. Famille indexée.

Définissons d'abord un cas particulier de famille indexée qui est celui des *suites :* à tout entier naturel n correspond un élément d'un ensemble E que l'on note x_n. Se donner une suite dans un ensemble E est donc se donner une application :

$$N \longrightarrow E.$$

De façon plus générale, I étant un ensemble quelconque qui sera l'ensemble des indices, se donner une famille d'éléments de E indexée par I, c'est se donner une application :

$$I \longrightarrow E$$

qui à tout $i \in I$ fait correspondre $x_i \in E$.

11. Généralisation des notions d'intersection et de réunion.

Soit $\mathcal{F}$ une famille de parties de E et A, son élément générique :

$$A \in \mathcal{F} \qquad \mathcal{F} \subset \mathcal{P}(E) \text{ ou } \mathcal{F} \in \mathcal{P}\mathcal{P}(E)$$

On considère une réunion et une intersection définies par :

$$\bigcup \{A \,;\, A \in \mathcal{F}\} = \{x \,;\, \exists A \in \mathcal{F},\ x \in A\},$$

$$\bigcap \{A \,;\, A \in \mathcal{F}\} = \{x \,;\, \forall A \in \mathcal{F},\ x \in A\}.$$

On peut aussi employer les notations :

$$\bigcup_{A \in \mathcal{F}} A \qquad \bigcap_{A \in \mathcal{F}} A$$

Exercice 12. — $\mathcal{F}$ et $\mathcal{G}$ étant 2 familles de parties de E démontrer :

$$\left[\bigcup \{A; A\in\mathcal{F}\}\right]\cup\left[\bigcup \{A; A\in\mathcal{G}\}\right]=\bigcup \{A; A\in \mathcal{F}\cup\mathcal{G}\}$$

$$\left[\bigcap \{A; A\in\mathcal{F}\}\right]\cap\left[\bigcap \{A; A\in\mathcal{G}\}\right]=\bigcap \{A; A\in \mathcal{F}\cup\mathcal{G}\}$$

$$\left[\bigcup \{A; A\in\mathcal{F}\}\right]\cap\left[\bigcup \{B; B\in\mathcal{G}\}\right]=\bigcup \{A\cap B; (A,B)\in \mathcal{F}\times\mathcal{G}\}$$

$$\left[\bigcap \{A; A\in\mathcal{F}\}\right]\cup\left[\bigcap \{B; B\in\mathcal{G}\}\right]=\bigcap \{A\cup B; (A,B)\in \mathcal{F}\times\mathcal{G}\}$$

La deuxième et la quatrième de ces formules peuvent être démontrées soit directement, soit comme formules duales de la première et de la troisième.

Exercice 13. — Soit une famille de parties de E, indexée par les éléments d'un produit cartésien I × J, X_{ij} un élément de cette famille, f étant une application de I dans J et $\mathcal{F}$ la famille de ces applications.

a) comparer :

$$\bigcap_{i\in I}\left[\bigcup_{j\in J} X_{ij}\right] \text{ et } \bigcup_{i\in J}\left[\bigcap_{i\in I} X_{ij}\right]$$

b) démontrer :

$$\bigcap_{i\in I}\left[\bigcup_{j\in J} X_{ij}\right] = \bigcup_{f\in\mathcal{F}}\left[\bigcap_{i\in I} X_{i f(i)}\right]$$

et en déduire la formule duale.

12. Relation d'équivalence.

On appelle *partition* d'un ensemble E une famille de sous-ensembles deux à deux disjoints et telle que leur réunion constitue tout l'ensemble, ou, ce qui revient au même, telle que tout élément de E puisse être « classé » dans un des sous-ensembles, c'est-à-dire appartienne à un sous-ensemble et à un seul.

π représente donc une partition de E si

$$A\in\pi,\ B\in\pi,\ A\neq B\Rightarrow A\cap B=\emptyset$$

$$\bigcup (A\ ;\ A\in\pi)=E.$$

Ceci posé, considérons la relation : *x et y appartiennent au même sous-ensemble de la partition.*

$$xRy \iff \exists A\in\pi \quad x\in A \quad y\in A.$$

On constate que cette relation jouit des propriétés suivantes :

1) Elle est *réflexive :* $\forall x\in E \quad xRx$,
(ceci découlant du fait que tout élément x appartient à un A).
2) Elle est *symétrique :* $xRy\Rightarrow yRx$.
3) Elle est *transitive :* $xRy,\ yRz\Rightarrow xRz$,
(ceci découlant du fait que tout x n'appartient qu'à un seul A).

Réciproquement : A toute relation réflexive, symétrique et transitive entre les éléments d'un ensemble correspond une partition de cet ensemble.

Soit E l'ensemble et R la relation satisfaisant aux trois conditions ci-dessus ; x étant un élément de E, on appelle *classe de x* (*modulo* R), et l'on note $\dot{x}$, l'ensemble :

$$\dot{x}=\{y\ ;\ xRy\} \qquad \dot{x}\in\mathcal{P}(E).$$

Pour montrer que l'ensemble des $\dot{x}$ constitue une partition, on doit montrer que la réunion des classes est E et que ces classes sont deux à deux disjointes, c'est-à-dire que :

$$\dot{x}\cap\dot{y}\neq\emptyset\Rightarrow\dot{x}=\dot{y}.$$

1) Tout x est classé puisque xRx, donc $x\in\dot{x}$ et la réunion des classes est bien E.

2) Soit : $z\in\dot{x}\cap\dot{y}$,
on a xRz et yRz, donc, grâce à la symétrie zRy, donc grâce à la transitivité xRy, donc $y\in\dot{x}$, et

$$\forall u\in\dot{y} \quad yRu \quad \text{donc } xRu \quad \text{donc } \dot{y}\subset\dot{x}.$$

On montrerait évidemment de même que $\dot{x}\subset\dot{y}$. D'où $\dot{x}=\dot{y}$.

Une relation réflexive, symétrique et transitive entre les éléments d'un ensemble est appelée une *relation d'équivalence*. Les classes ci-dessus définies sont nommées *classes d'équivalence* (*modulo* R) et l'ensemble des classes est dit *ensemble quotient de* E *par* R et est noté :

$$E/R.$$

L'application

$$E\longrightarrow E/R$$

qui à x fait correspondre $\dot{x}$ est très importante. Elle est dite *application canonique* de E sur E/R.

Exemples :

R	Une classe d'équivalence définit :
égalité de fractions,	un nombre rationnel,
parallélisme de droites (*),	une direction de droite,
équipollence de vecteurs,	un vecteur libre,
isométrie des ensembles plans.	une « figure indéformable » par glissement et retournement dans son plan au sens de la géométrie intuitive.

13. Factorisation canonique d'une application.

Soit d'abord une application :

$$E\xrightarrow{f}F$$

et soit la relation définie sur E :

$$xRy\iff f(x)=f(y).$$

Cette relation est évidemment réflexive, symétrique et transitive ; c'est une relation d'équivalence et chaque classe est constituée par l'ensemble des éléments de E qui ont même image dans F.

(*) Pour que le parallélisme jouisse de la propriété de réflexivité et, sans restriction, de celle de transitivité, il est nécessaire de prendre le terme parallèles dans le sens de « confondues ou n'ayant aucun point commun » (pour les droites d'un même plan).

Exercice 14. — Soit S une relation d'équivalence sur F ; on définit R sur E par

$$xRy \iff f(x)\ S\ f(y)$$

Montrer que R est une relation d'équivalence.

Remplaçons maintenant F par $f(E)$, ce qui revient à supprimer dans F les éléments qui ne sont pas images d'éléments de E, et considérons l'application :

$$E \xrightarrow{g} f(E)$$

remplaçant ainsi f par une application surjective. On peut ensuite considérer l'application canonique de $f(E)$ dans F qui à tout élément de $f(E)$ fait correspondre lui-même (cette application est évidemment injective ; plus généralement, on appelle injection canonique d'une partie A d'un ensemble F dans F l'application :

$$A \longrightarrow F$$

qui, à tout $x \in A$, fait correspondre x lui-même).

On peut donc écrire :

$$f = i \circ g$$

pour traduire le schéma :

$$E \xrightarrow{g} f(E) \xrightarrow{i} F.$$

Revenons à la relation d'équivalence $xRy \iff f(x) = f(y)$. Elle pourra aussi bien être définie par $g(x) = g(y)$. Mais cette fois, g étant surjective, tout élément u de $f(E)$ est image d'une classe d'équivalence dans E, donc correspond à un élément de l'ensemble quotient E/R qui peut donc être représenté par $f^{-1}(u)$. L'application g peut alors être décomposée de la façon suivante :

$$E \longrightarrow f(E) \longrightarrow F.$$

L'application $E \longrightarrow E/R$ est l'application canonique de l'ensemble E sur l'ensemble quotient. L'application $E/R \longrightarrow f(E)$ qui à tout $\dot{x} = f^{-1}(u)$ fait correspondre u est une bijection. Finalement, on écrira :

avec :

$$f = i \circ \psi \circ \varphi$$

$$\begin{array}{ccccc} E & \xrightarrow{\varphi} & E/R & \xrightarrow{\psi} & f(E) \xrightarrow{i} F \\ x & \longrightarrow & \dot{x} & \longrightarrow & u \longrightarrow u \\ & & \text{surjection canonique} & & \text{bijection} \quad \text{injection canonique} \end{array}$$

Exemple : E étant une boule fermée (ensemble des points M tels que OM ⩽ rayon), f sera la projection orthogonale de E sur un plan F ; $f(E)$ sera le disque fermé, projection de E. Un élément $\dot{x}$ est un segment de la boule perpendiculaire à F. Ces éléments se correspondent biunivoquement avec la trace de leur support sur F.

14. Relations d'ordre.

Il s'agit de donner une formulation mathématique des idées de « avant » et « après ». Or, dans le langage courant, b est avant a et c est avant b entraîne que c est avant a. La relation « b est avant a » devra donc être transitive. Ensuite, « a est avant b » et « b est avant a » s'excluent dans le langage courant. Ici, les mathématiciens considèrent deux cas différents suivant que les deux affirmations précédentes s'excluent ou bien sont compatibles dans le seul cas où a et b sont égaux. Nous poserons donc les définitions suivantes :

Relation d'ordre strict. Une relation R sur un ensemble E est dite relation d'ordre strict si :

$\forall (a, b, c) \in E^2 \quad aRb \Rightarrow$ non bRa.
$\forall (a, b) \in E \quad aRb \Rightarrow$ non bRa.

Relation d'ordre. Une relation R sur un ensemble E est dite relation d'ordre (sans épithète) si :

$\forall (a, b, c,) \in E^3 \quad aRb$ et $bRc \Rightarrow aRc$ transitivité.
$\forall a \in E \quad aRa$, réflexivité,
$\forall (a, b) \in E^2 \quad aRb$ et $bRa \Rightarrow a = b$,

cette dernière propriété étant parfois nommée « antisymétrie ». Bien entendu, les relations $a < b$ et $a \leqslant b$ entre nombres réels sont respectivement une relation d'ordre strict et une relation d'ordre.

Nous n'avons pas supposé pour le moment que pour tout couple (x, y) d'éléments de E on avait :

$$xRy \text{ ou } yRx.$$

Si, au contraire :

$\forall (x, y) \in E^2$, xRy ou yRx,

on dit que R est une *relation d'ordre total.*

Dans le cas contraire, on dit que R est une *relation d'ordre partiel* ou une relation d'ordre (sans épithète).

Les exemples précédemment cités sur l'ensemble des réels étaient des relations d'ordre total. On peut au contraire citer les exemples suivants d'ordre partiel.

1) Sur l'ensemble des lieux appartenant au bassin d'un fleuve, la relation « être en aval de » :

Rouen est en aval d'Auxerre,

mais Auxerre et Troyes ne sont pas comparables.

2) Sur l'ensemble $\mathcal{P}(E)$, l'inclusion $A \subset B$ est de même une relation d'ordre partiel.

Notations. Nous conviendrons de noter une relation d'ordre :

$$a \prec b,$$

ce que nous lirons a est avant b, ou a est antérieur à b, ou b est après a, ou b est postérieur à a.

R étant une relation d'ordre, la relation S définie par :

$$aSb \iff bRa$$

est évidemment aussi une relation d'ordre. Chacun des deux ordres est dit *dual* de l'autre.

Autre exemple : Ordres sur le plan.

Nous citerons 2 relations d'ordre possibles sur le plan rapporté à 2 axes de coordonnées, c'est-à-dire sur R^2 (R représentant l'ensemble des réels) :

1) Etant donnés les points M (x_1, x_2) et P (y_1, y_2), on posera :

$$M \prec P \iff \begin{cases} x_1 \leqslant y_1 \\ x_2 \leqslant y_2. \end{cases}$$

Exercice 14. — Soit S une relation d'équivalence sur F ; on définit R sur E par

$$xRy \iff f(x)\ S\ f(y)$$

Montrer que R est une relation d'équivalence.

Remplaçons maintenant F par $f(E)$, ce qui revient à supprimer dans F les éléments qui ne sont pas images d'éléments de E, et considérons l'application :

$$E \xrightarrow{g} f(E)$$

remplaçant ainsi f par une application surjective. On peut ensuite considérer l'application canonique de $f(E)$ dans F qui à tout élément de $f(E)$ fait correspondre lui-même (cette application est évidemment injective ; plus généralement, on appelle injection canonique d'une partie A d'un ensemble F dans F l'application :

$$A \longrightarrow F$$

qui, à tout $x \in A$, fait correspondre x lui-même).

On peut donc écrire :

$$f = i \circ g$$

pour traduire le schéma :

$$E \xrightarrow{g} f(E) \xrightarrow{i} F.$$

Revenons à la relation d'équivalence $xRy \iff f(x) = f(y)$. Elle pourra aussi bien être définie par $g(x) = g(y)$. Mais cette fois, g étant surjective, tout élément u de $f(E)$ est image d'une classe d'équivalence dans E, donc correspond à un élément de l'ensemble quotient E/R qui peut donc être représenté par $f^{-1}(u)$. L'application g peut alors être décomposée de la façon suivante :

$$E \longrightarrow f(E) \longrightarrow F.$$

L'application $E \longrightarrow E/R$ est l'application canonique de l'ensemble E sur l'ensemble quotient. L'application $E/R \longrightarrow f(E)$ qui à tout $\dot{x} = f^{-1}(u)$ fait correspondre u est une bijection. Finalement, on écrira :

$$f = i \circ \psi \circ \varphi$$

avec :

$$\begin{array}{ccccc} E & \xrightarrow{\varphi} & E/R & \xrightarrow{\psi} & f(E) \xrightarrow{i} F \\ x & \longrightarrow & \dot{x} & \longrightarrow & u \longrightarrow u \\ & & \text{surjection canonique} & & \text{bijection} \qquad \text{injection canonique} \end{array}$$

Exemple : E étant une boule fermée (ensemble des points M tels que OM ⩽ rayon), f sera la projection orthogonale de E sur un plan F ; $f(E)$ sera le disque fermé, projection de E. Un élément $\dot{x}$ est un segment de la boule perpendiculaire à F. Ces éléments se correspondent biunivoquement avec la trace de leur support sur F.

14. Relations d'ordre.

Il s'agit de donner une formulation mathématique des idées de « avant » et « après ». Or, dans le langage courant, b est avant a et c est avant b entraîne que c est avant a. La relation « b est avant a » devra donc être transitive. Ensuite, « a est avant b » et « b est avant a » s'excluent dans le langage courant. Ici, les mathématiciens considèrent deux cas différents suivant que les deux affirmations précédentes s'excluent ou bien sont compatibles dans le seul cas où a et b sont égaux. Nous poserons donc les définitions suivantes :

Relation d'ordre strict. Une relation R sur un ensemble E est dite relation d'ordre strict si :

$\forall (a, b, c) \in E^2 \quad aRb \Rightarrow$ non bRa.
$\forall (a, b) \in E \quad aRb \Rightarrow$ non bRa.

Relation d'ordre. Une relation R sur un ensemble E est dite relation d'ordre (sans épithète) si :

$\forall (a, b, c,) \in E^3 \quad aRb$ et $bRc \Rightarrow aRc$ transitivité.
$\forall a \in E \quad aRa$, réflexivité,
$\forall (a, b) \in E^2 \quad aRb$ et $bRa \Rightarrow a = b$,

cette dernière propriété étant parfois nommée « antisymétrie ». Bien entendu, les relations $a < b$ et $a \leqslant b$ entre nombres réels sont respectivement une relation d'ordre strict et une relation d'ordre.

Nous n'avons pas supposé pour le moment que pour tout couple (x, y) d'éléments de E on avait :

$$xRy \text{ ou } yRx.$$

Si, au contraire :

$\forall (x, y) \in E^2$, xRy ou yRx,

on dit que R est une *relation d'ordre total.*

Dans le cas contraire, on dit que R est une *relation d'ordre partiel* ou une relation d'ordre (sans épithète).

Les exemples précédemment cités sur l'ensemble des réels étaient des relations d'ordre total. On peut au contraire citer les exemples suivants d'ordre partiel.

1) Sur l'ensemble des lieux appartenant au bassin d'un fleuve, la relation « être en aval de » :

Rouen est en aval d'Auxerre,

mais Auxerre et Troyes ne sont pas comparables.

2) Sur l'ensemble $\mathcal{P}(E)$, l'inclusion $A \subset B$ est de même une relation d'ordre partiel.

Notations. Nous conviendrons de noter une relation d'ordre :

$$a \prec b,$$

ce que nous lirons a est avant b, ou a est antérieur à b, ou b est après a, ou b est postérieur à a.

R étant une relation d'ordre, la relation S définie par :

$$aSb \iff bRa$$

est évidemment aussi une relation d'ordre. Chacun des deux ordres est dit *dual* de l'autre.

Autre exemple : Ordres sur le plan.

Nous citerons 2 relations d'ordre possibles sur le plan rapporté à 2 axes de coordonnées, c'est-à-dire sur R^2 (R représentant l'ensemble des réels) :

1) Etant donnés les points M (x_1, x_2) et P (y_1, y_2), on posera :

$$M \prec P \iff \begin{cases} x_1 \leqslant y_1 \\ x_2 \leqslant y_2. \end{cases}$$

Il s'agit d'une relation d'ordre partiel. M est avant tous les points du quadrant I, après tous ceux du quadrant III, n'est pas comparable à ceux des quadrants II et IV (fig. 2).

Remarquons que ce qu'on nomme en probabilités, la valeur de la fonction de répartition F (x_1, x_2) est la probabilité pour qu'un point soit antérieur au point M (x_1, x_2), c'est-à-dire pour que ce point tombe dans le quadrant III.

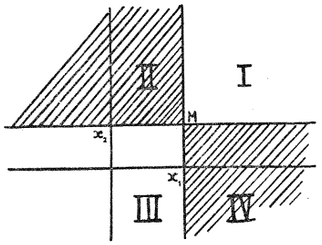


FIG. 2

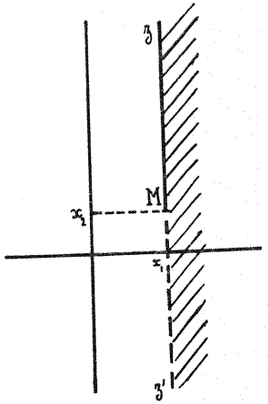


FIG. 3

2) On posera :

$$M \prec P \iff x_1 < y_1 \quad \text{ou} \quad x_1 = y_1,\ x_2 \leqslant y_2.$$

Cette fois, il s'agit d'une relation d'ordre total. Les points antérieurs à M sont ceux du demi-plan situé à gauche de $z'z$ et ceux de la demi-droite M z' ; ceux du demi-plan de droite et ceux de la demi-droite M z sont après M (fig. 3).

Cet ordre, qui est fondé sur le même principe que celui adopté pour les mots d'un dictionnaire, est dit *ordre lexicographique*.

Remarque. De la même façon que nous venons d'ordonner le plan R^2, on peut ordonner un espace à n dimensions R^n par l'un ou l'autre des procédés que nous venons d'indiquer.

Exercice 15. — Relation d'ordre sur l'ensemble $\mathcal{R}$ des relations d'équivalence sur un ensemble E. On dira :
$R_1 \prec R_2$ (on lira ici « R_1 est plus fine que R_2 ») si $xR_1y \Rightarrow xR_2y$.
Montrer qu'il s'agit bien d'une relation d'ordre ; qu'en résulte-t-il pour les graphes des relations R_1 et R_2 ?

Exercice 16. — F étant un ensemble ordonné montrer que le premier procédé utilisé pour le plan permet de munir d'un ordre l'ensemble $\mathcal{F}$ (E, F) des applications de E dans F.

Autre exemple : Un mobile étant en mouvement sur un axe Ox, on considère « l'espace temps » qui est ici le plan rapporté aux axes Ot et Ox où l'on considère le point M de coordonnées : le temps t et l'abscisse x du mobile à l'instant t. On suppose que la vitesse du mobile doit rester

en valeur absolue inférieure à une valeur fixe c (vitesse de la lumière dans la théorie de la relativité). Un point M (t_0, x_0) étant donné, on peut considérer le passé et le futur du mobile, ceux-ci étant définis respectivement comme l'ensemble des positions que le point M peut avoir occupées avant et celles qu'il est susceptible d'occuper après.

Ceux-ci sont respectivement les points de 2 angles opposés par le sommet, définis par les 2 droites de coefficient angulaire c et $-c$ passant par M_0 (fig. 4).

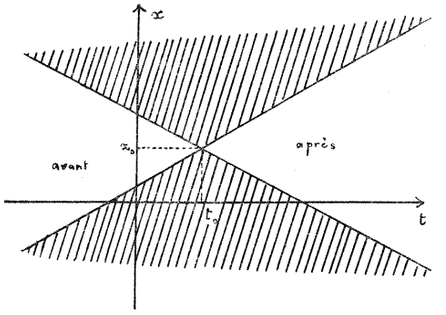


FIG. 4

15. Eléments remarquables dans les ensembles ordonnés.

Majorant d'un ensemble. E étant ordonné par une relation d'ordre $\prec$, considérons un sous-ensemble A $\in \mathcal{P}$ (E). a sera dit élément majorant de A si :

$$\forall x \in A \quad x \prec a.$$

Si un ensemble a des majorants, on dit qu'il est majoré.

E étant le plan ordonné par la première des relations d'ordre considérées ci-dessus, le point a majore tout ensemble tel que A, formé de points du 3e quadrant défini par a. Au contraire, la bande de plan B n'admet aucun majorant.

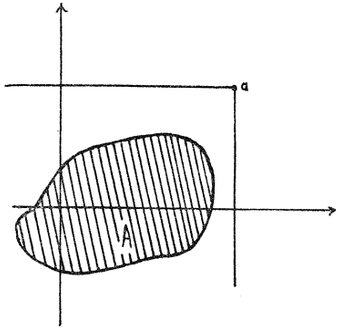


FIG. 5

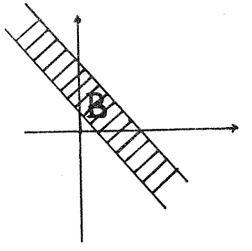


FIG. 6

Remarque. On définit de façon analogue un *minorant.*

Plus grand élément d'un ensemble. On nomme ainsi un majorant qui appartient à l'ensemble. Si un tel élément existe, il est unique. En effet, si a et b étaient deux tels éléments, la définition appliquée à a entraînerait $b \prec a$ et appliquée à b entraînerait $a \prec b$; donc : $b = a$.

Remarque. On définira de façon analogue un plus petit élément.

Elément maximal. Un élément a d'un ensemble A est dit maximal si

$$a \in A,\ x \in A \qquad a \prec x \quad \Rightarrow \quad x = a,$$

autrement dit si a est après tous les éléments qui lui sont comparables. Un plus grand élément est maximal mais la réciproque est fausse. Par exemple, sur la bande de la figure précédente, tout élément de la frontière supérieure est maximal sans être plus grand élément.

Remarque. On définira de façon analogue un élément *minimal.*

Borne supérieure d'un ensemble. On dit qu'un ensemble admet une borne supérieure si l'ensemble de ses majorants admet un plus petit élément (désignée en anglais par l. u. b. lowest upper bound). On appelle de même *borne inférieure* (en anglais g. l. b. greatest lower bound) le plus grand élément de l'ensemble des minorants.

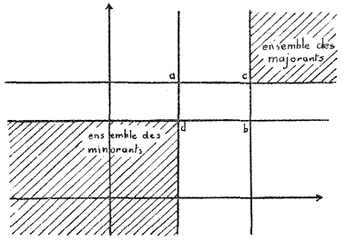


FIG. 7

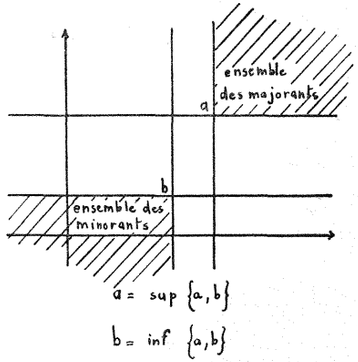


FIG. 8

Notations. Les bornes supérieures et inférieures d'un ensemble A seront notées :

$$\sup A \quad \text{et} \quad \inf A.$$

Dans le cas particulier d'un ensemble constitué de 2 éléments $\{a, b\}$, on pourra employer les notations :

$$a \vee b = \sup \{a, b\} \text{ et } a \wedge b = \inf \{a, b\}.$$

Ces signes, déformations des signes de réunion et d'intersection, se justifient par le fait que dans le cas de l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble ordonné par la relation d'inclusion :

$$\sup (A, B) = A \cup B \quad \inf (A, B) = A \cap B,$$

puisque :

$$C \subset A,\ C \subset B \Rightarrow C \subset A \cap B$$

et :

$$C \supset A,\ C \supset B \Rightarrow C \supset A \cup B.$$

Exemple : Dans le plan ordonné par la première de nos relations d'ordre, l'ensemble de 2 éléments admet toujours une borne supérieure et une borne inférieure. En effet, l'ensemble des majorants d'un point est l'ensemble des points du quadrant I (relatif à ce point). L'ensemble des majorants de l'ensemble constitué de 2 points a et b est donc l'intersection de 2 quadrants I. Il est facile de vérifier que dans tous les cas cette intersection est un quadrant qui a son sommet pour plus petit élément. Les circonstances sont analogues pour l'ensemble des minorants (fig. 7 et 8).

16. Treillis.

Quand un ensemble ordonné est tel que toute partie $\{a, b\}$ formée de 2 éléments admet une borne supérieure et une borne inférieure, on dit qu'il forme un treillis (en anglais lattice) ou encore qu'il est *réticulé.*

Remarquons qu'un ensemble muni d'un ordre total forme toujours un treillis. Des cas plus intéressants sont fournis par des ensembles munis d'un ordre partiel qui aient une structure de treillis.

Exemples : 1) Le plan muni de la première de nos structures d'ordre, comme on vient de le montrer.

2) $\mathcal{P}(E)$ ordonné par l'inclusion est un treillis, comme nous l'avons vu aussi ci-dessus.

3) Sur l'ensemble des entiers naturels, la relation

$$a|b \ (a \text{ divise } b)$$

est une relation d'ordre partiel et la borne supérieure de 2 nombres est leur P.P.C.M., la borne inférieure est le P.G.C.D.

Exercice 17. — Montrer que l'ensemble des relations d'équivalence muni de l'ordre indiqué dans l'exercice 15 forme un treillis.

Exercice 18. — Considérons une relation réflexive, transitive, mais pour laquelle on peut avoir xRy et yRx avec $y \neq x$.

Considérons la relation S définie par :

$$xSy \iff xRy \text{ et } yRx$$

Montrer que S est une relation d'équivalence et que sur E/S on peut définir un ordre naturellement associé à la relation R.

CHAPITRE II : GROUPES

§ 1. — GENERALITES SUR LES STRUCTURES ALGEBRIQUES.

On dit qu'on a muni un ensemble d'une structure algébrique quand on a défini des opérations (ou loi de composition) entre les éléments de cet ensemble.

1. Loi de composition interne.

A tout couple d'éléments de E, la loi fait correspondre un élément de E (*). Donner la loi est donc donner une application

$$E^2 \longrightarrow E$$

Exemples : 1) L'addition et la multiplication sont des lois de composition interne sur l'ensemble des réels.

2) La réunion et l'intersection sont 2 lois de composition interne sur l'ensemble des parties d'un ensemble.

3) Les lois

$$(a, b) \to a \wedge b \text{ et } (a, b) \to a \vee b$$

sont 2 lois de composition internes sur un treillis. Le 2e exemple n'est d'ailleurs qu'un cas particulier du 3e.

2. Loi de composition externe. Il s'agit cette fois d'une application

$$E \times F \longrightarrow E$$

L'exemple le plus simple est celui du produit d'un vecteur par un scalaire qui, au couple formé d'un vecteur et d'un scalaire, fait correspondre un vecteur.

L'ensemble F est dit ensemble des *opérateurs*.

Remarque. — Le produit scalaire, faisant correspondre un nombre à un couple de vecteurs, apparaît comme une application

$$E^2 \longrightarrow \mathbf{R}$$

où E désigne l'ensemble des vecteurs libres de l'espace. Ce n'est donc pas une loi de composition.

3. Propriétés des lois de composition interne. Nous conviendrons de noter par

$$a \top b$$

le composé de 2 éléments a et b.

(*) On peut aussi considérer des lois non partout définies, c'est-à-dire qui, à certains couples d'éléments de E (mais pas forcément à tous), fassent correspondre un élément de E. Une telle loi est, pour utiliser la terminologie introduite en I, 2, 3, une fonction de E^2 dans E et non une application. C'est le cas de la soustraction dans N. Nous ne ferons ici aucune étude générale de telles lois, car dans les cas élémentaires, le progrès a consisté à utiliser la possibilité (qui n'existe pas dans le cas général) de remplacer l'ensemble E par un ensemble F plus vaste sur lequel la loi non partout définie de E a été prolongée en une loi partout, définie sur F.

Commutativité. Si

$$\forall (a, b) \in E^2 \qquad a \top b = b \top a,$$

on dit que la loi est commutative.

Les opérations de l'algèbre élémentaire sont commutatives, mais les exemples de lois non commutatives sont nombreux : produit de 2 transformations en géométrie ; composition des permutations de n éléments, c'est-à-dire des applications bijectives d'un ensemble de n éléments sur lui-même.

Associativité. Si

$$\forall (a, b, c) \in E^3 \qquad (a \top b) \top c = a \top (b \top c),$$

on dit que la loi est associative. Dans ce cas, l'élément obtenu sera noté :

$$a \top b \top c.$$

Observons qu'une puissance d'un élément (en adoptant le langage de l'opération multiplication) n'est un élément défini sans autre convention que si la loi considérée est associative.

Exemple de loi non associative : celle qui, à un couple de points de l'espace, fait correspondre leur milieu.

Elément neutre. Soit toujours une loi de composition interne sur un ensemble E. On appelle élément neutre un élément e tel que :

$$\forall a \in E \quad a \top e = e \top a = a.$$

Exemples : 0 est élément neutre pour l'addition dans R.
1 est élément neutre pour la multiplication dans R,
la transformation identique pour le produit de transformations dans R^2 ou R^3.

Si $\forall a \in E$ $e' \top a = a$, e' est dit *élément neutre à gauche.*
Si $\forall a \in E$ $a \top e'' = a$, e'' est dit *élément neutre à droite.*

S'il existe un élément neutre à gauche et un élément neutre à droite, ils sont égaux ; en effet :

$e' \top e'' = e'$ puisque e' est neutre à gauche
$e' \top e'' = e''$ ..... e'' ..... droite.

Elément inverse. L'élément inverse d'un élément a est l'élément a' défini, s'il existe, par :

$$a \top a' = a' \top a = e.$$

Il est noté a^{-1}. On dit alors que a est inversible.

§ 2. PROPRIETES GENERALES DES GROUPES. HOMOMORPHISMES

Dans tout ce qui suit, il s'agira de loi de composition interne sur un ensemble. Sauf avis contraire, la loi de composition sera notée multiplicativement, ab désignant le composé de a et de b pris dans l'ordre indiqué.

1. Axiomes de la structure de groupe.

On dit qu'un ensemble G *est un groupe pour une loi de composition donnée sur un ensemble si :*

1) *La loi est associative :*

$$\forall (a, b, c) \in G^3 \quad (a\,b)\,c = a\,(b\,c).$$

2) *Il existe un élément neutre bilatère :*

$$\forall a \in G \quad a\,e = e\,a = a.$$

3) *Tout élément admet un inverse bilatère :*

$$\forall a \in G \qquad \exists a^{-1} \in G \qquad a\,a^{-1} = a^{-1}\,a = e.$$

Ces axiomes de la structure de groupe sont plus forts qu'il n'est nécessaire. On peut en effet montrer que le système d'axiomes que nous allons considérer maintenant entraîne le système précédent et, en conséquence, suffit à établir une structure de groupe. Ce système est le suivant :

1) *La loi est associative.*

2 *bis*) *Il existe un élément neutre à droite e :*

$$\forall a \in G \quad a\,e = a.$$

3 *bis*) *Tout élément a un inverse à droite :*

$$\forall a \in G \quad \exists a' \in G \quad a\,a' = e.$$

Montrons d'abord que a' est inverse à gauche, c'est-à-dire que $a'\,a = e$. Pour cela, considérons l'inverse à droite de a' que l'on note a'' :

$$a'\,a'' = e,$$

et calculons $a'\,a$ en utilisant la propriété d'associativité :

$$a'a = a'ae = a'a\,(a'a'') = a'\,(aa')\,a'' = a'ea'' = a'a'' = e.$$

Montrons ensuite que e est élément neutre à gauche en montrant que $ea = a$ pour tout a :

$$ea = (aa')\,a = a\,(a'a) = ae = a.$$

Remarque. L'inverse d'un produit de plusieurs facteurs est le produit des inverses des facteurs pris dans l'ordre opposé :

$$(abc)^{-1} = c^{-1}\,b^{-1}\,a^{-1}.$$

En effet :

$$(abc)\,(c^{-1}\,b^{-1}\,a^{-1}) = ab\,(cc^{-1})\,b^{-1}\,a^{-1}$$
$$= abe\,b^{-1}\,a^{-1} = a(bb^{-1})\,a^{-1} = aea^{-1} = aa^{-1} = e.$$

2. Applications du groupe sur lui-même et résolution des équations dans un groupe.

Considérons les produits de tous les éléments d'un groupe G par un élément a de G, ce qui veut dire que nous considérons l'application :

$$x \in G \longrightarrow ax \in G.$$

Cette application est injective, car $ax = ay \Rightarrow a^{-1}\,ax = a^{-1}\,ay$, donc $x = y$.

Elle est surjective car :

$$\forall b \in G \quad \exists x \text{ tel que } ax = b \text{ c'est } x = a^{-1}b.$$

Elle est donc bijective.

Cette propriété fondamentale est illustrée par les tables de Pythagore du groupe, tableaux à double entrée où figurent les composés de 2 éléments.

La propriété précédente s'exprime immédiatement par le fait que dans la colonne a figure une fois et une seule chaque élément du groupe. La même propriété peut être démontrée pour les lignes en considérant une multiplication à droite et l'application :

$$x \longrightarrow xa.$$

Remarque. Le fait que l'application $x \longrightarrow ax$ (ou l'application

$x \longrightarrow xa$) soit injective peut s'énoncer : une égalité entre éléments d'un groupe du type $ax = ay$ (ou $xa = ya$) est *simplifiable* :

$$ax = ay \Rightarrow x = y \qquad xa = ya \Rightarrow x = y.$$

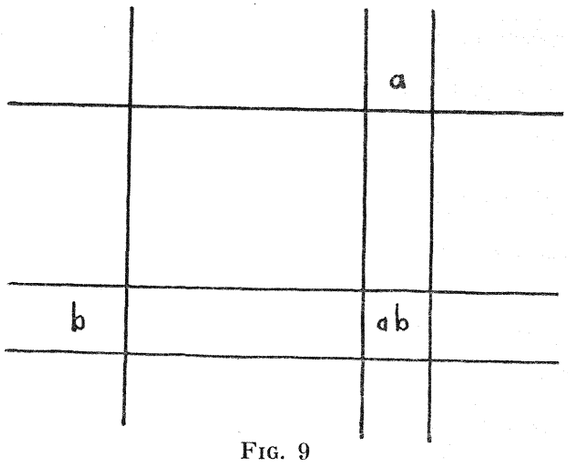


FIG. 9

Il résulte de ce qui précède que l'équation

$$ax = b,$$

où a, b appartiennent au groupe et où x doit lui appartenir, admet la solution

$$x = a^{-1}b$$

et n'admet qu'elle. Il en sera de même pour l'équation

$$xa = b$$

qui admet la solution

$$x = ba^{-1}$$

et n'admet qu'elle.

On reconnaît les formules classiques : $a + x = b$ a pour solution $x =$ opposé de $a + b$ dans **R** (ensemble des réels) qui forme un groupe par rapport à l'addition, et $ax = b$ a pour solution $x = \frac{1}{a} \times b$ dans $\mathbf{R} - \{0\}$ ou dans $\mathbf{R}^+ - \{0\}$ (ensemble des réels > 0) qui forment des groupes par rapport à la multiplication.

Réciproquement. Si, sur un ensemble E, *est définie une loi de composition associative telle que :*

$$\forall a \quad \forall b \in E \quad \exists x \in E \quad ax = b \quad \exists y \in E \quad ya = b,$$

cette loi est une loi de groupe.

En effet, montrons l'existence d'un élément neutre à droite. La première hypothèse permet d'affirmer qu'il existe e_a tel que $ae_a = a$.

Il suffit alors de montrer que $\forall b \quad be_a = b$.

Pour cela, utilisons la 2e hypothèse et soit y tel que $ya = b$:

$$be_a = yae_a = y(ae_a) = ya = b.$$

Donc, e_a que nous notons dorénavant e est neutre à droite. Ensuite, tout élément a un inverse à droite puisque $ax = e$ admet une solution. Les axiomes faibles énoncés ci-dessus sont donc vérifiés.

Remarque. L'unicité des solutions des équations $ax = b$ et $ya = b$ n'a pas été supposée. Elle résulte de l'existence de ces solutions pour les équations relatives à tous les couples (a, b).

3. Partie stable d'un ensemble.

Soit E un ensemble muni d'une loi de composition. Un sous-ensemble $A \subset E$ est dit *stable* pour la loi de composition si

$$\forall (a, b) \in A^2 \qquad ab \in A.$$

Exemple : N (ensemble des entiers naturels) est une partie stable de Z (ensemble des entiers relatifs) pour l'addition. Une loi de composition interne est alors définie sur A. C'est une application

$$A \times A \longrightarrow A$$

qui est la restriction à $A \times A$ de la loi de E qui est une application de $E \times E$ dans E.

Cette loi de composition est dite la loi *induite* sur A par la loi de composition sur E.

Il sera commode à ce propos d'introduire ce qu'on appelle :

4. Extension à $\mathcal{P}(E)$ d'une loi de composition sur E.

Si $A \subset E$, $B \subset E$, on appellera composé de A et de B l'ensemble défini par :

$$AB = \{c \ ; \ \exists a \in A, b \in B, c = ab\}.$$

Cet ensemble ne doit pas être confondu avec le produit cartésien $A \times B$ qui est défini dès que A et B le sont et indépendamment de toute loi de composition. Un élément ab de AB est le composé des 2 éléments du couple (a, b) de $A \times B$. Toutefois, la notation A^2 désigne suivant le cas AA ou $A \times A$ (on précisera si une confusion est à craindre).

En particulier, on considérera l'ensemble des produits par un élément fixe a de tous les éléments d'une partie B de E :

$$\{a\}B = \{c \ ; \ \exists b \in B \quad c = ab\}$$

que, par abus de langage, on notera plus simplement aB. De même, on note par A^{-1} l'ensemble des inverses des éléments de A :

$$A^{-1} = \{b \ ; \ \exists a \in A \quad c = ab\}.$$

Remarquons les règles de calcul suivantes qui sont évidentes :

$$A \subset B \Rightarrow AC \subset BC,$$
$$A \subset B \Rightarrow A^{-1} \subset B^{-1}.$$

Si A^{-1} n'est pas vide, $e \in AA^{-1}$, mais généralement $\{e\} \neq AA^{-1}$.

Avec ces notations, une partie stable est caractérisée par $AA \subset A$.

5. Sous-groupes.

Si g est une partie stable d'un groupe G qui soit un groupe pour la loi induite, g est dit un sous-groupe de G.

Exemples : Dans Z, l'ensemble des entiers pairs (noté 2Z) est un sous-groupe pour l'addition. Dans le groupe des déplacements plans, les translations forment un sous-groupe.

Si g est un sous-groupe de G, en tant que partie stable il satisfait à :

$$gg \subset g$$

et, en tant que groupe, à :

$$g^{-1} \subset g.$$

Réciproquement, si g est une partie stable de B satisfaisant à :

$$g^{-1} \subset g \quad \text{et} \quad g^2 \subset g,$$

g est un sous-groupe. En effet :

$$a \in g \quad a^{-1} \in g^{-1} \subset g \qquad aa^{-1} = e \in g^2 \subset g,$$

donc e appartient à g et puisque $g^{-1} \subset g$, tous les inverses des éléments de g sont donc dans g.

Remarquons enfin qu'en appliquant les règles de calcul signalées ci-dessus, on trouve que $g^{-1} \subset g$ entraîne $g \subset g^{-1}$, donc $g = g^{-1}$ et que $\{e\} \subset g$ entraîne $eg = g \subset gg$ qui, avec $gg \subset g$, donne $gg = g$.

Exercice 19. — Quelles sont toutes les structures de groupe pour des ensembles de $n = 2, 3, 4, 5...$ éléments.

	e	a
e	e	a
a	a	e

Pour $n = 2$, on trouve une seule structure possible dont la table de Pythagore est donnée ci-contre. Tous les groupes à 2 éléments ont donc la même structure. Nous dirons qu'ils sont isomorphes. Rentrent, entre autres, dans ce schéma :

loi de composition	élément e	élément a
« règle des signes » somme	signe + classe des entiers $\equiv 0$ (mod 2)	signe — classe des entiers $\equiv 1$ (mod 2)
produit	classe des entiers $\equiv 1$ (mod 3)	classe des entiers $\equiv 2$ (mod 3)
produit (ou composition) de transformations	identité	symétrie par rapport à une droite fixe.
produit de permutations	identité	permutation $\begin{pmatrix} 1, 2 \\ 2, 1 \end{pmatrix}$

Nous allons définir de façon plus générale :

6. Isomorphisme des groupes.

On dit que 2 groupes G_1 et G_2 dotés de lois de composition notées respectivement $\perp$ et $\top$ sont isomorphes quand :

1) il existe une bijection φ de G_1 sur G_2 ;

2) $\forall (x, y) \in G_1^2 \quad \varphi(x \perp y) = \varphi(x) \top \varphi(y)$ (1).

Ceci peut être schématisé de la façon suivante :

Les lois de composition sont les applications :

$$G_1^2 \xrightarrow{\perp} G_1 \qquad G_2^2 \xrightarrow{\top} G_2.$$

D'autre part, on peut faire correspondre G_1^2 à G_2^2 par l'application désignée par $\varphi \times \varphi$:

$$(x, y) \in G_1^2 \xrightarrow{\varphi \times \varphi} (\varphi(x), \varphi(y)) \in G_2^2$$

On peut alors faire le diagramme :

$$\begin{array}{ccc} G_1^2 & \xrightarrow{\varphi \times \varphi} & G_2^2 \\ {\scriptstyle \perp}\downarrow & & \downarrow{\scriptstyle \top} \\ G_1 & \xrightarrow{\varphi} & G_2 \end{array}$$

L'égalité (1) exprime alors qu'on peut aller de G_1^2 à G_2 par un chemin ou par l'autre sans que le résultat en soit modifié. Un tel diagramme est dit commutatif.

Exemples : G_1 et G_2 étant R^+ et les lois de groupe $\top$ et $\perp$ la multiplication, φ étant l'application

$$x \xrightarrow{\varphi} \sqrt{x},$$

l'isomorphisme exprime simplement que le produit des racines (chemin de droite) est égal à la racine du produit (chemin de gauche).

G_1 étant R^+, la loi $\perp$ la multiplication, G_2 étant R, la loi $\top$ l'addition, φ étant l'application :

$$x \longrightarrow \operatorname{Log} x,$$

l'isomorphisme exprime que le Log du produit (chemin de gauche) est égal à la somme des Log (chemin de droite).

Un isomorphisme de G sur lui-même est appelé *automorphisme.* Notons que parmi eux il y a l'identité.

Automorphismes intérieurs. Soit un groupe G non commutatif et soit a un élément de G. Considérons l'application :

$$x \longrightarrow axa^{-1}$$

qui n'est pas une identité si a ne commute pas avec tous les éléments de G ($\exists b \in G \quad ab \neq ba$).

Cette application définit un isomorphisme de G sur lui-même appelé automorphisme intérieur. En effet :

1) Cette application est bijective. Elle est en effet la composée des 2 applications :

$$x \longrightarrow ax = y \quad \text{et} \quad y \longrightarrow y a^{-1},$$

dont nous avons montré plus haut qu'elles étaient bijectives.

2) Cette application est compatible avec la loi de composition du groupe. En effet, elle fait correspondre :

$$x \longrightarrow a\,x\,a^{-1}$$
$$y \longrightarrow a\,y\,a^{-1}$$
$$xy \longrightarrow a\,(xy)\,a^{-1}.$$

Or $(a\,x\,a^{-1})\,(a\,y\,a^{-1}) = ax\,(a^{-1}a)\,y\,a^{-1} = a\,(xy)\,a^{-1}$.

L'image du composé (par la loi de groupe) est donc bien le composé des images.

Nous allons considérer maintenant l'ensemble A des automorphismes intérieurs d'un groupe G et montrer que cet ensemble a une structure de groupe.

Soient φ_a et φ_b les éléments de A, automorphismes définis comme précédemment, respectivement à l'aide des éléments a et b. Le composé $\varphi_b \circ \varphi_a$ de deux automorphismes intérieurs est un automorphisme intérieur. En effet, faisons subir à un élément x l'application composée ci-dessus. Il vient :

$$x \xrightarrow{\varphi_a} axa^{-1} \xrightarrow{\varphi_b} b\,(axa^{-1})\,b^{-1} = (ba)x(a^{-1}b^{-1}) = (ba)x(ba)^{-1},$$

ab étant un élément de G, on peut donc écrire :

$$\varphi_b \circ \varphi_a = \varphi_{ba}.$$

Cette loi de composition est associative en vertu même de cette égalité, car :

$$\varphi_c \circ (\varphi_b \circ \varphi_a) = \varphi_c \circ \varphi_{ba} = \varphi_{cba} = \varphi_{cb} \circ \varphi_a = (\varphi_c \circ \varphi_b) \circ \varphi_a,$$

cette loi possède un élément neutre car φ_e est l'identité.

D'autre part, tout automorphisme intérieur a un inverse qui est l'application réciproque :

$$\varphi_a^{-1} = \varphi_{a^{-1}},$$

car $\varphi_a \circ \varphi_a^{-1} = \varphi_{a\,a^{-1}} = \varphi_e$, d'après (1).

A forme donc un groupe, la loi de composition interne étant la composition (au sens des applications). Nous pouvons nous demander si ce groupe est isomorphe à A.

L'application

$$a \in \mathrm{G} \longrightarrow \varphi_a \in \mathrm{A}$$

est compatible avec les lois de composition définies sur G et A en vertu de l'égalité (1). Il resterait donc seulement à établir que cette application est bijective et, comme elle est évidemment surjective, il faudrait seulement montrer qu'elle est injective.

Exercice 20. — On montrera qu'elle l'est si, et seulement si G ne possède aucun élément $\neq e$ qui commute avec tous les autres.

7. Homomorphisme des groupes.

Soit une application φ d'un groupe G dans un ensemble E muni d'une loi de composition et qui jouit de la même propriété qu'un isomorphisme, exprimée avec les mêmes notations par :

$$\varphi\,(x \perp y) = \varphi(x)\ \mathbf{T}\ \varphi(y), \qquad (1)$$

mais que, cette fois, on ne suppose plus bijective.

Une telle application est appelée homomorphisme de G dans E.

Si l'application φ est injective, on parlera d'homomorphisme injectif ou monomorphisme.

Si l'application φ est surjective, on parlera d'homomorphisme surjectif ou épimorphisme.

Soit donc une application d'un groupe G (loi de composition notée $\perp$) dans un ensemble E muni d'une loi de composition (notée $\mathbf{T}$), et utilisons la factorisation canonique des applications vue au chapitre premier.

$$\mathrm{G} \xrightarrow[\text{appl. canonique}]{\varphi} \mathrm{G/R} \xrightarrow[\text{bijection}]{h} f\,(\mathrm{G}) \xrightarrow[\text{inject. canonique}]{i} \mathrm{E}$$
$$f = i \circ h \circ \varphi$$

et supposons que f soit un homomorphisme, ce qui se traduit par l'hypothèse :

$$f(x)\ \mathbf{T}\ f(y) = f(x \perp y) \quad (1),$$

et voyons ce qui en résulte pour les divers éléments de cette factorisation.

D'abord, f (G) est une partie stable de E et est un groupe. En effet, l'hypothèse (1) montre que f (G) est une partie stable pour $\mathbf{T}$, puisque 2 éléments quelconques de f (G) sont de la forme $f(x)$ et $f(y)$ et que leur composé par $\mathbf{T}$ est l'élément $f(x \perp y)$ qui, par définition, appartient aussi à f (G). L'associativité de la loi induite par $\mathbf{T}$ sur f (G) découle immédiatement de celle de la loi $\perp$.

Cette même égalité (1) montre que :

$$f(x)\ \mathbf{T}\ f(e) = f(x \perp e) = f(x),$$

donc que $f(e)$ est élément neutre pour $\mathbf{T}$.

Enfin, $f(x^{-1}{}_{\perp})$, $x^{-1}{}_{\perp}$ désignant l'inverse de x pour la loi de composition sur G, est l'inverse $[f(x)]^{-1}{}_{\mathbf{T}}$ pour la loi sur E, puisque :

$$f(x \perp x^{-1}) = f(e) = f(x)\ \mathbf{T}\ f(x^{-1}).$$

Donc, f (G) est un groupe.

Si maintenant nous négligeons E pour ne considérer que f (G), nous sommes devant un homomorphisme surjectif qui se factorise comme suit :

$$\mathrm{G} \xrightarrow{\varphi} \mathrm{G/R} \xrightarrow{h} f\,(\mathrm{G}).$$
$$x \longrightarrow \dot{x} \longrightarrow f(x) = h(\dot{x}).$$

Les 2 ensembles G et f (G) sont munis de leur loi de composition ; quant à l'ensemble G/R jusqu'ici non structuré, nous allons le munir d'une loi de composition que nous noterons $*$ et qui sera déterminée par la condition que h soit un isomorphisme, ce qui n'est possible que d'une seule manière. Voyons ce qui en résulte pour φ. Nous avons donc le schéma :

$$\begin{array}{ccccc} \mathrm{G} & \xrightarrow{\varphi} & \mathrm{G/R} & \xrightarrow{h} & f\,(\mathrm{G}) \\ \perp & & * & \text{isomorphisme} & \mathbf{T} \end{array}$$

Le fait que f soit un homomorphisme s'écrit :

$$\forall (x, y) \in \mathrm{G}^2 \qquad f(x \perp y) = f(x)\ \mathbf{T}\ f(y)$$

ou

$$h(\widehat{x \perp y}) = h(\dot{x})\ \mathbf{T}\ h(\dot{y}) \qquad (1)$$

Le fait que h doive être un isomorphisme donne de même :

$$h(\dot{x} * \dot{y}) = h(\dot{x})\ \mathbf{T}\ h(\dot{y}) \qquad (2).$$

En rapprochant (1) de (2), on trouve que la loi $*$ satisfait à :

$$\widehat{x \perp y} = \dot{x} * \dot{y} \qquad \forall (x, y) \in \mathrm{G}^2$$

c'est-à-dire

$$\varphi(x \perp y) = \varphi(x) * \varphi(y),$$

c'est-à-dire que φ est un homomorphisme. L'ensemble G/R muni de cette loi de composition est l'image homomorphe du groupe G par l'applica-

tion canonique $G \longrightarrow G/R$. C'est donc un groupe que l'on qualifie de *groupe quotient de* G.

Et, en conclusion, *un homomorphisme d'un groupe* G *dans un ensemble* E *quelconque muni d'une loi de composition peut se factoriser en :*

1) *un homomorphisme surjectif de* G *sur un groupe quotient* G/R ;
2) *un isomorphisme de* G/R *sur* $f(G)$;
3) *un homomorphisme injectif d'un sous-groupe* $f(G)$ *de* E *dans* E.

On obtiendra donc tous les groupes auxquels G peut être homomorphe en déterminant tous les groupes quotients G/R auxquels il peut être homomorphe. Cherchons à caractériser ces groupes quotients.

La relation R est définie par :

$$x R y \Longleftrightarrow f(x) = f(y),$$

ce qui peut aussi s'écrire, en revenant pour les deux lois de groupe à la notation multiplicative et en désignant par e_1, l'élément neutre du groupe $G_1 = f(G)$:

$$f(x)\,[f(y)]^{-1} = e_1.$$

Or, en vertu de l'homomorphisme, cette dernière relation peut s'écrire :

$$f(xy^{-1}) = e_1,$$

c'est-à-dire que :

$$xy^{-1} \in \overset{-1}{f}(e_1),$$

$\overset{-1}{f}(e_1)$ étant l'image réciproque de e_1 dans G ; cette image est appelée le *noyau* de l'homomorphisme. Il peut se faire que $\overset{-1}{f}(e_1)$ se réduise à e :

$$\overset{-1}{f}(e_1) = \{e\}.$$

Cette condition est évidemment réalisée quand l'homomorphisme :

$$G_1 \xrightarrow{f} G$$

de G_1 sur G est un isomorphisme. Et, réciproquement, elle est suffisante pour que f soit un isomorphisme. En effet, elle exprime que seul e a pour image e_1, donc qu'on ne peut avoir $f(x) = f(y)$, c'est-à-dire $f(xy^{-1}) = e_1$, sans avoir $xy^{-1} = e$, c'est-à-dire $x = y$, autrement dit que :

$$f(x) = f(y) \Rightarrow x = y,$$

donc que f est injective, ce qui suffit ici pour qu'elle soit un isomorphisme.

Revenons maintenant au cas général où le noyau :

$$\overset{-1}{f}(e_1) \neq \{e\},$$

et remarquons que le sous-ensemble $\overset{-1}{f}(e_1)$ de G, que nous désignons par g, est un sous-groupe. En effet :

$$u \in g \quad v \in g \Longleftrightarrow f(u) = e_1 \quad f(v) = e_1,$$
$$\text{donc :} \quad f(uv) = f(u)f(v) = e_1,$$
$$\text{donc :} \quad uv \in g.$$

D'autre part : $e \in g$

Enfin : $f(u^{-1}) = [f(u)]^{-1}$.

(Ne pas confondre : $[f(u)]^{-1}$ avec $\overset{-1}{f}(u)$).

$$f(u^{-1}) = [f(u)]^{-1} = e_1{}^{-1} = e_1)$$

donc, $g^{-1} \subset g$, donc tout élément de g a son inverse dans g et g est bien un sous-groupe.

Il résulte donc de la théorie précédente que la relation R, qui donnait un groupe quotient G/R homomorphe à G et dont on a vu qu'elle pouvait s'écrire :

$$xy^{-1} \in \overset{-1}{f}(e_1),$$

prend la forme :

$$xy^{-1} \in g,$$

g étant un sous-groupe de G. De plus, ce sous-groupe n'est pas quelconque. Il est *invariant* dans tous les automorphismes intérieurs de G. Soit, en effet :

$$\varphi_a(x) = axa^{-1}.$$

Si : $x \in g$, $\varphi_a(x) \in g$, car $f(\varphi_a(x)) = f(a)e_1f(a^{-1}) = f(a)\,[f(a)]^{-1} = e_1$,

donc : $\varphi_a(g) \subset g$, ce qu'on exprime par :

$$\forall a \in G \qquad aga^{-1} \subset g$$

aga^{-1} représentant l'ensemble des axa^{-1} quand x décrit g. Mais, ceci étant valable pour tout a, on peut écrire :

$$a^{-1}ga \subset g,$$

ce qui entraîne (après multiplication à gauche par a, et à droite par a^{-1}) :

$$g \subset aga^{-1},$$

donc :

$$g = aga^{-1}.$$

Un sous-groupe qui jouit de cette propriété est dit *sous-groupe invariant* ou *sous-groupe distingué* (en allemand Normalteiler). Remarquons que si G est commutatif, tous ses sous-groupes sont invariants.

On convient de noter G/g l'ensemble quotient G/R muni de la loi de composition qu'on vient de lui attribuer, c'est-à-dire le groupe quotient. Et nous énoncerons :

Tout groupe qui peut être image homomorphe d'un groupe G *est isomorphe à un groupe quotient* G/g, *g étant un sous-groupe invariant.*

Exercice 21. — 1° Démontrer que l'ensemble des éléments c d'un groupe G qui commutent avec tous les éléments du groupe forment un sous-groupe invariant C que l'on appelle le centre du groupe.

2° Reprenant l'exercice 20, montrer que quand $G \neq \{e\}$, l'ensemble A des automorphismes intérieurs est isomorphe au groupe G/C.

Etude de la réciproque. A tout sous-groupe invariant g de G, peut-on associer un groupe quotient G/g qui soit image homomorphe de G ?

Soit donc un sous-groupe g. Sans utiliser pour le moment le fait qu'il est invariant, nous pouvons montrer que la relation R définie par :

$$x R y \Longleftrightarrow xy^{-1} \in g$$

est une relation d'équivalence. En effet :

1) $e = xx^{-1} \in g$,
2) $xy^{-1} \in g \Rightarrow (xy^{-1}) = yx^{-1} \in g$,
3) $xy^{-1} \in g,\ yz^{-1} \in g \Rightarrow xy^{-1}yz^{-1} = xz^{-1} \in g$.

Pour cette relation d'équivalence, la classe d'équivalence de x est :

$$\mathring{x} = \{y,\ xRy\} = \{y\ ;\ xy^{-1} \in g\} = \{y\ ;\ yx^{-1} \in g\},$$

cette dernière formule exprimant que x est l'ensemble des y tels que :

$$\exists u \in g \qquad y = ux,$$

c'est-à-dire l'ensemble des ux pour u décrivant g ; on écrira :

$$\dot{x} = gx$$

et on appellera cet ensemble une *classe à droite* relativement à g. On peut définir de même la relation d'équivalence S par :

$$xSy \Longleftrightarrow y^{-1}x \in g \Longleftrightarrow x^{-1}y \in g.$$

La classe d'équivalence de x est alors xg, *classe à gauche* relativement à g.

La définition d'un sous-groupe invariant :

$$(xgx^{-1} = g \Longleftrightarrow xg = gx),$$

n'est donc autre que : sous-groupe dont les classes à gauche sont identiques aux classes à droite, c'est-à-dire, encore, sous-groupe tel que les deux relations d'équivalence R et S soient confondues.

Il s'agit de montrer maintenant que l'on peut munir G/R d'une loi de composition (notée *), telle que l'application canonique :

$$\varphi : G \longrightarrow G/R$$

soit un homomorphisme (G/R, image homomorphe d'un groupe, sera alors un groupe).

Le fait que φ soit un homomorphisme impose comme loi de composition :

$$\dot{x} * \dot{y} = \dot{\widehat{xy}}.$$

Ceci ne sera possible que si u décrivant toute la classe $\dot{x}$ et v toute la classe $\dot{y}$, le produit uv appartient toujours à la classe de xy, c'est-à-dire si :

$$gx\ gy \subset gxy$$

$gx\ gy$ contenant d'ailleurs $gx\ ey$, c'est-à-dire gxy, l'inclusion précédente est équivalente à l'égalité :

$$gx\ gy = gxy \qquad (1).$$

Pour un sous-groupe quelconque, il n'en est généralement pas ainsi. Mais si g est invariant :

$$gx = xg,$$

ce qui veut dire :

$$\forall u \in g \quad \exists u' \in g \quad \text{tel que } ux = xu',$$

et, dans ce cas, on peut écrire :

$$gxgy = ggxy = gxy,$$

ce calcul symbolique traduisant la succession d'égalité entre éléments :

$$\forall (uv) \in g^2 \quad uxvy = xu'vy = x(u'v)y = xwy = w'xy$$
$$\text{avec } w = u'v \in g \quad \text{et } w' \in g.$$

L'égalité (1) est donc démontrée moyennant l'hypothèse que g est invariant ; G/R est dans ce cas identique à G/S ; on note cet ensemble quotient, auquel on vient de donner la structure de groupe G/g, et il est l'image homomorphe de G.

En rapprochant ce résultat de celui démontré page 45, nous pouvons énoncer :

Pour que l'espace quotient G/R ($xRy \Longleftrightarrow xy^{-1} \in g$) *puisse être image homomorphe de* G, *il faut et il suffit que* g *soit un sous-groupe invariant de* G.

Ou encore :

On obtient tous les groupes qui peuvent être images homomorphes de G en prenant tous les groupes isomorphes aux groupes quotients G/g, g décrivant l'ensemble des sous-groupes invariants de G.

Exercice 22. — Relation d'équivalence régulière.

On peut établir la théorie précédente en se posant le problème : G étant un groupe, R une relation d'équivalence sur G, que doit être R pour que l'on puisse définir sur l'espace quotient G/R une loi de composition telle que l'application canonique de G sur G/R soit un homomorphisme ?

1) On établira que la condition nécessaire et suffisante pour qu'il en soit ainsi est que R soit régulière par rapport à la loi de composition sur G, c'est-à-dire que :

$$\forall a \in G \quad xRy \Rightarrow axRay \text{ et } xaRya$$

2) On montrera (sans utiliser la théorie du cours) que cette condition est équivalente à : il existe un sous-groupe invariant g de G, tel que :

$$xRy \Longleftrightarrow xy^{-1} \in g$$

8. Quelques exemples de groupes et de sous-groupes.

I. Z, *ensemble des entiers relatifs, forme un groupe pour l'addition.*

Cherchons tous ses sous-groupes qui seront tous invariants, ce groupe étant commutatif.

Un tel sous-groupe contient obligatoirement des nombres positifs et des nombres négatifs. Soit a le plus petit des nombres > 0 d'un sous-groupe g ; le sous-groupe contient tous les nombres de la forme :

$$\underbrace{a + a + \ldots + a}_{n \text{ termes}},$$

que l'on convient de noter na. (Si $n < 0$, on pose $na = -[(-n)a]$).

Soit b un autre élément du sous-groupe et supposons que :

$$na < b < (n+1)a,$$

on pourra alors écrire : $b = na + r \qquad 0 < r < a.$

$b \in g$, $na \in g$, donc $r \in g$, ce qui est contraire à l'hypothèse que a est le plus petit élément positif de g. g ne possède donc aucun élément b qui ne soit pas de la forme na ; g est l'ensemble des na et sera noté $a\mathbf{Z}$.

Ensemble quotient. Les classes d'équivalence seront de la forme :

$$\dot{x} = x + a\mathbf{Z}.$$

Il y aura a classes distinctes : $\dot{0}, \dot{1}, \ldots, \dot{\widehat{a-1}}$.

Z étant abélien, Z/aZ est image homomorphe de Z : $\dot{\alpha} + \dot{\beta} = \dot{\widehat{\alpha + \beta}}$.

Le groupe Z/aZ est le groupe additif des entiers modulo a, noté aussi $\mathbf{Z}_a$.

II. *Groupe additif des réels.* Il possède de nombreux sous-groupes. Z en est un ; R/Z est formé des classes $\dot{x} = x + \mathbf{Z}$, c'est-à-dire des nombres réels modulo 1. Ce groupe noté T_1 est appelé parfois tore à une dimension. Il est isomorphe au groupe des réels modulo 2π, dont chaque classe est l'ensemble des abscisses curvilignes d'un point d'un cercle de rayon 1.

III. *Groupe $\mathcal{D}$ des isométries du plan.* Contrairement aux précédents, ce groupe n'est pas abélien et tous ses sous-groupes ne sont pas invariants. (Par exemple, les rotations de centre fixe forment un sous-groupe qui n'est pas invariant).

Parmi les sous-groupes invariants, on peut citer :

$\mathcal{D}$, groupe des déplacements (ou isométries positives), le produit

$I \circ D \circ I^{-1}$ étant un déplacement si D est un déplacement, que I soit un déplacement ou une isométrie négative. Il y a deux classes : $\mathcal{D}$ (déplacements) et $\mathcal{A}$ (isométries négatives).

$\mathcal{I} / \mathcal{D}$ est donc un groupe à 2 éléments isomorphe à tous les groupes à 2 éléments (voir II, 2, 5).

$\mathcal{T}$, groupe des translations est un sous-groupe invariant de $\mathcal{D}$, car $D \circ T \circ D^{-1}$ est une translation si T en est une, comme on le montre en géométrie. $\mathcal{D} / \mathcal{T}$ est constitué des classes $D \circ \mathcal{T}$, D étant une rotation donnée d'angle α ; or, on sait que l'ensemble des déplacements $D \circ \mathcal{T}$ constitue l'ensemble des rotations d'angle α. $\mathcal{D} / \mathcal{T}$ est donc isomorphe au groupe des réels modulo 2π : $\mathbf{R}/2\pi\mathbf{Z}$, c'est-à-dire à T_1.

Remarque. Observons qu'ici $\mathcal{T}$ est aussi un sous-groupe invariant de $\mathcal{I}$. En effet, on peut décomposer I en $S \circ D_1$ et I^{-1} en $D_2 \circ S$, S étant une symétrie et D_1 et D_2 des déplacements d'angles opposés, ce qui donne :

$$I \circ T \circ I^{-1} = S \circ (D_1 \circ T \circ D_2) \circ S = S \circ T' \circ S = T'',$$

T'' étant la translation de vecteur symétrique de celui de T' dans la symétrie S.

Ici donc :

$\mathcal{D}$	est sous-groupe invariant	de	$\mathcal{I}$
$\mathcal{T}$	——	——	$\mathcal{D}$
$\mathcal{T}$	——	——	$\mathcal{I}$

Il faudrait se garder de croire que cette circonstance est générale : un sous-groupe invariant d'un sous-groupe invariant de G pouvant ne pas être un sous-groupe invariant de G.

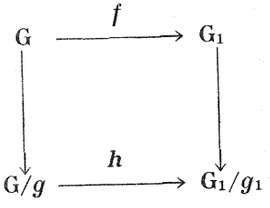
IV. *Ensemble $\mathcal{C}$ des fonctions continues réelles sur* $[a, b]$. Cet ensemble forme un groupe par rapport à l'addition, la fonction $f + g$ étant définie par :

$$\forall x \in [a, b] \quad (f + g)(x) = f(x) + g(x),$$

l'élément neutre étant la fonction partout nulle que nous notons 0.

On peut considérer le sous-groupe des fonctions nulles en x_0, soit $\mathcal{I}_{x_0}$. Le groupe étant abélien, ce sous-groupe est invariant. La classe d'une fonction f est formée de $f + \mathcal{I}_{x_0}$, c'est-à-dire de toutes les fonctions qui, en x_0, prennent la même valeur que f. Le groupe quotient $\mathcal{C} / \mathcal{I}_{x_0}$ est donc isomorphe au groupe additif des réels.

Exercice 23. — Soient G et G_1, deux groupes tels qu'il existe un homomorphisme f de G *sur* G_1.



a) g_1 étant un sous-groupe invariant de G_1, montrer que $g = f^{-1}(g_1)$ est un sous-groupe invariant de G_1 et que les groupes quotients G/g et G_1/g_1 sont isomorphes.

b) Soient deux groupes G et G_1 et un homomorphisme f de G sur G_1, g et g_1, deux sous-groupes invariants de G et G_1 respectivement et tels que $f(g) \subset g_1$.

Montrer qu'il existe un homomorphisme h de G/g dans G_1/g_1 tel que le diagramme précédent soit commutatif.

Exercice 24.

a) Dans un groupe G d'ordre $2n$, tout sous-groupe g d'ordre n est invariant.

b) Soit G d'ordre $2n$ possédant deux sous-groupes g_1 et g_2 d'ordre n, tels que $g_1 \cap g_2 = \{e\}$. Montrer que ceci n'est possible que pour une seule valeur de n et une seule structure de G. Combien G possède-t-il de sous-groupes d'ordre n ?

c) Dans le cas général d'un groupe G d'ordre $2n$ ayant deux sous-groupes distincts d'ordre n, se ramener au cas précédent par un passage convenable au quotient. Que peut-on en déduire pour l'ordre et la structure de G ?

9. Générateurs d'un groupe. Groupes cycliques.

Remarquons d'abord que l'intersection d'une famille de sous-groupes est un sous-groupe. Soit alors A une partie de G et considérons tous les sous-groupes qui contiennent A, leur intersection g est le plus petit sous-groupe de G contenant A. On dit que *g est engendré par* A ou que A *est un ensemble de générateurs de g.*

Supposons alors que A ne contienne qu'un élément a. Le plus petit sous-groupe contenant a est celui des puissances de a :

$$\ldots \; a^{-n} \ldots\ldots a^{-1} \ldots\ldots e \;\; a \;\; a^2 \ldots\ldots a^m \ldots$$

Un tel groupe g engendré par un seul élément est dit *monogène.* Puisque $a^n . a^m = a^{n+m}$, l'application :

$$n \in \mathbf{Z} \longrightarrow a^n$$

est un homomorphisme de $\mathbf{Z}$ sur g ; g est donc isomorphe à un groupe quotient de $\mathbf{Z}$, c'est-à-dire soit à $\mathbf{Z}$ lui-même, soit à $\mathbf{Z}/n\mathbf{Z}$.

Dans le premier cas, qui se présente quand aucune puissance de a n'est égale à l'élément neutre, g est un groupe *monogène infini.* Dans le 2e cas, $a^n = e$, $a^{n+1} = a \ldots a^{n+m} = a^m$, le groupe a un nombre fini d'éléments, n. On dit qu'il est *cyclique.* n (qui est la plus petite puissance de a telle que $a^n = e$, et qui est l'ordre du groupe g) est dit ordre de l'élément a dans le groupe G.

Or, si G est lui-même fini, et si g est un quelconque de ses sous-groupes, toute classe modulo g (classe à gauche par exemple) a autant d'éléments que g lui-même. Il en résulte que l'ordre de G est un multiple de l'ordre de g. *Dans un groupe fini, l'ordre d'un sous-groupe est un diviseur de l'ordre du groupe.*

Si, en particulier, g est le groupe cyclique engendré par un élément a, le théorème précédent prouve que l'ordre d'un élément divise l'ordre du groupe (tout élément a un ordre fini dans un groupe fini). Il en résulte que $a^m = e$ avec $m | n$, n étant l'ordre du groupe, donc $a^n = e$.

Dans un groupe fini d'ordre n, $a^n = e$, a étant un élément quelconque du groupe.

Remarque. Si p est premier, les entiers différents de 0, de $\mathbf{Z}_p$, forment pour la multiplication un groupe à $p - 1$ éléments, comme nous le

verrons ultérieurement. Appliquée à ce groupe, la propriété précédente n'est autre que le théorème de Fermat ($a^{p-1} \equiv 1 \bmod p$).

Exercice 25. —

a) A étant une partie non vide d'un groupe G, montrer qu'il existe une plus petite partie stable $\tilde{A}$ contenant A et que :

$$\tilde{A} = \bigcup \{ A^n,\ n \in \mathbf{N} \}$$

b) Déterminer le plus petit sous-groupe contenant A.

Exercice 26. —

1) A et B étant deux sous-groupes d'un groupe G, on considère le plus petit sous-groupe g contenant $A \cup B$. Montrer que tout élément de g est obtenu comme produit d'une suite finie d'éléments appartenant alternativement à A et à B.

2) Montrer que la condition nécessaire et suffisante pour que g soit égal à AB est que l'on ait $AB = BA$ (les deux groupes A et B seront dits permutables).

Qu'en résulte-t-il si un des groupes A, B est invariant ?

3) Déduire de ce qui précède que l'ensemble des sous-groupes d'un groupe G ordonné par inclusion est un treillis.

Même question pour l'ensemble des sous-groupes invariants d'un groupe G. (Préciser ce que sont alors $g_1 \wedge g_2$ et $g_1 \vee g_2$).

4) Montrer que si A et B sont deux sous-groupes permutables et C un sous-groupe contenant A, A est permutable avec $B \cap C$ et qu'on a

$$A(B \cap C) = C \cap AB$$

En déduire que le treillis des sous-groupes invariants d'un groupe est modulaire ce qui signifie que

$$A \prec C \Rightarrow A \vee (B \wedge C) = (A \vee B) \wedge C$$

On pourra montrer à ce propos que, dans tout treillis, l'implication suivante est vraie

$$A \prec C \Rightarrow A \vee (B \wedge C) \prec (A \vee B) \wedge C$$

5) Montrer que si A est un sous-groupe invariant de G et B un sous-groupe quelconque de G, les deux groupes $B/A \cap B$ et AB/A sont isomorphes.

Exercice 27. —

1) Soit G un groupe abélien d'ordre n fini. Montrer que l'on peut trouver une suite finie de sous-groupes $U_1, U_2, \ldots U_k$ tels que

$$e \subset U_1 \subset U_2 \subset U_3 \ldots \subset U_{k-1} \subset U_k \subset G$$

et tels que U_1, U_2/U_1, $U_3/U_2 \ldots$ U_k/U_{k-1}, G/U_k soient cycliques.

2) On dit qu'un groupe G est simple lorsqu'il n'a pas de sous-groupes non triviaux (autres que G et $\{e\}$).

Montrer qu'on peut résoudre la question précédente en imposant aux groupes quotients U_{i+1}/U_i d'être cycliques simples.

Montrer qu'alors le nombre des groupes U_i et l'ensemble des ordres des groupes quotients est unique pour toutes les décompositions de ce type. (Autrement dit, pour deux décompositions différentes, on obtiendra comme groupe quotient les mêmes groupes cycliques simples, mais pas forcément dans le même ordre).

§ 3. PRODUIT CARTESIEN DE GROUPES

1. Soient 2 groupes G_1 et G_2 et soit :

$$G = G_1 \times G_2 = \{ (a_1, a_2)\ ;\ a_1 \in G_1 \quad a_2 \in G_2 \},$$

leur produit cartésien. Nous pouvons doter ce produit cartésien d'une structure algébrique en définissant l'opération :

$$(a_1, a_2) \,.\, (b_1, b_2) = (a_1 b_1, a_2 b_2).$$

Il est immédiat que $G_1 \times G_2$ forme un groupe pour cette opération, l'élément neutre étant (e_1, e_2) si e_1 et e_2 désignent respectivement les éléments neutres de G_1 et G_2.

Exemples : 1) $\mathbf{R} \times \mathbf{R}$ où $\mathbf{R}$ est le groupe additif des réels forme un groupe :

$$(x, y) + (x', y') = (x + x', y + y'),$$

cette opération n'est autre que la somme vectorielle.

Ceci s'étend sans difficulté à $\mathbf{R}^n$.

2) $\mathbf{R} \times T_1$ représente les points d'un cylindre.

3) $T_1 \times T_1$ représente les points d'un tore.

Sur l'une comme sur l'autre de ces surfaces, comme précédemment sur le plan $\mathbf{R}^2$, l'opération de groupe est une loi de composition qui, à deux points, fait correspondre un point.

Ces groupes sont les mêmes que ceux de transformations dans lesquels les points considérés sont les homologues d'un point origine fixe : groupe des translations dans le plan $\mathbf{R}^2$, groupe des déplacements hélicoïdaux sur le cylindre $\mathbf{R} \times T_1$ et sur le tore T_1^2 le groupe des doubles rotations, en désignant par double rotation le produit d'une rotation sur le parallèle par une rotation sur le méridien.

Chacun de ces groupes est commutatif comme les groupes facteurs du produit, $\mathbf{R}$ ou T_1.

G_1 et G_2 sont isomorphes à des sous-groupes invariants de $G_1 \times G_2$.

Cette proposition s'établit facilement. En effet, considérons :

$$g_1 = \{ (a_1, e_2)\ ;\ a_1 \in G_1 \}.$$

Il est immédiat que g_1 est un sous-groupe de $G_1 \times G_2$ et que l'application

$$\begin{aligned} g_1 &\longrightarrow G_1 \\ (a_1, e_2) &\longrightarrow a_1 \end{aligned}$$

est un isomorphisme. Il reste donc seulement à vérifier que g_1 est invariant. Or,

$$\begin{aligned} (b_1, b_2) \,.\, (a_1, e_2) \,.\, (b_1^{\,1}, b_2^{-1}) &= (b_1 a_1 b_1^{-1}, b_2 e_2 b_2^{-1}) \\ &= (a_1', e_2) \in g_1. \end{aligned}$$

Cherchons alors ce qu'on peut dire du groupe quotient G/g_1. Ses éléments, classes de G modulo g_1, sont de la forme :

$$g_1 (b_1, b_2) = \{ (a_1 b_1, e_2 b_2)\ ;\ a_1 \in G_1 \} = \{ (c_1, b_2)\ ;\ c_1 \in G_1 \}.$$

Une classe est donc constituée par tous les couples dont la deuxième composante b_2 a une valeur fixe et dont la première décrit tout le groupe.

L'isomorphisme

$$\begin{aligned} G/g_1 &\longrightarrow G_2 \\ \overline{(b_1, b_2)} &\rightarrow b_2 \end{aligned}$$

est alors évident. Chacun des groupes facteurs du produit $G = G_1 \times G_2$ est donc isomorphe au groupe quotient de G par un groupe isomorphe à l'autre.

Il ne faudrait pas croire qu'il s'agit là d'une propriété générale. Il est, en général, faux que G soit isomorphe au produit $G/g \times g$, g étant

un quelconque sous-groupe invariant de G. Il résulte en effet du raisonnement précédent que, pour qu'il en soit ainsi, il serait nécessaire que G/g soit aussi isomorphe à un sous-groupe invariant de G. Or, il n'en est généralement pas ainsi. (Dans **Z**, par exemple, tous les sous-groupes sont infinis et tous les groupes quotients sont finis. Un groupe quotient de **Z** ne peut donc être isomorphe à un sous-groupe de **Z**, sauf pour les cas triviaux où le sous-groupe est $\{0\}$ ou **Z** : **Z** est trivialement isomorphe au produit cartésien de **Z** par $\{0\}$.

2. Produit direct.

Si $G = G_1 \times G_2$, tout élément a de G est de la forme (a_1, a_2) avec $a_1 \in G_1$, $a_2 \in G_2$, et peut s'écrire : $a = (a_1, e_2)(e_1, a_2)$, c'est-à-dire, en faisant intervenir les deux sous-groupes g_1 et g_2 de G respectivement isomorphes à G_1 et G_2, que tout élément de G s'exprime comme le produit d'un élément de g_1 par un élément de g_2.

On a donc : $G = g_1 g_2$ et G est le produit des deux sous-groupes g_1 et g_2 (ici non plus, au sens de produit cartésien, mais au sens de l'opération sur les parties du groupe G).

L'étude précédente a fait apparaître un certain nombre de propriétés de g_1 et g_2 :

1) $\forall x \in G$, la factorisation $x = x_1x_2$ avec $x_1 \in g_1$, $x_2 \in g_2$ est unique.

2) $\forall x_1 \in g_1, \quad \forall x_2 \in g_2, \quad x_1x_2 = x_2x_1$.

En effet $(a_1, e_2)(e_1, a_2) = (a_1, a_2) = (e_1, a_2)(a_1, e_2)$.

3) $g_1 \cap g_2 = \{e\}$.

4) g_1 et g_2 sont invariants.

On peut alors se poser le problème suivant : un groupe G étant le produit (pour l'opération sur l'ensemble de ses parties) de deux de ses sous-groupes g_1 et g_2, est-il isomorphe à leur produit cartésien ? Lorsqu'il en sera ainsi, on dira que G est le *produit direct* de ses deux sous-groupes g_1 et g_2.

Sous l'hypothèse initiale H ($G = g_1g_2$), les quatre conditions énoncées ci-dessus apparaissent comme nécessaires. Mais elles ne sont pas indépendantes. On a, en effet :

Sous l'hypothèse H, les implications suivantes ont lieu entre les quatre conditions énoncées ci-dessus :

$1 \Longleftrightarrow 3$; $2 \Rightarrow 4$; 3 et $4 \Rightarrow 2$ et par suite (1 et 2) $\Longleftrightarrow$ (3 et 4).

Démonstration. $1 \Rightarrow 3$. Si $g_1 \cap g_2$ contenait un élément $u \neq e$, cet élément admettrait les deux factorisations $u = ue = eu$.

$3 \Rightarrow 1$. Si $x = x_1x_2 = y_1y_2$, on en déduit $y_1^{-1}x_1 = y_2x_2^{-1} = e$ si g_1 et g_2 n'ont en commun que e, et par suite $x_1 = y_1$, $x_2 = y_2$.

$2 \Rightarrow 4$. Soit $u_1 \in g_1$, et considérons xu_1x^{-1} où $x \in G$. On peut écrire $x = x_2x_1$ et $x\,u_1\,x_1^{-1} = x_2x_1u_1x_1^{-1}x_2^{-1}$. Or, $x_1u_1x_1^{-1} \in g_1$.

D'après 2, on a donc :

$$x_2(x_1u_1x_1^{-1})x_2^{-1} = (x_1u_1x_1^{-1})x_2x_2^{-1} = x_1u_1x_1^{-1} \in g_1.$$

Même démonstration pour g_2.

(3 et 4) $\Rightarrow$ 2. Considérons $x_1x_2(x_2x_1)^{-1} = u = x_1x_2x_1^{-1}x_2^{-1}$; g_2 étant invariant, $x_1x_2x_1^{-1} \in g_2$, d'où $u \in g_2$. De même, g_1 étant invariant, $x_2x_1x_2^{-1} \in g_1$, d'où $u \in g_1$. De $g_1 \cap g_2 = \{e\}$ résulte $u = e$, c'est-à-dire $x_1x_2 = x_2x_1$.

Sous l'hypothèse H, les conditions 1 et 2 impliquent que :

$$G \approx g_1 \times g_2.$$

Soit, en effet, $x = x_1x_2$, la factorisation unique de l'élément $x \in G$; elle permet de définir une bijection φ de G sur $g_1 \times g_2$:

$$\varphi(x) = (x_1, x_2).$$

Reste à vérifier que φ est un homomorphisme. Si y est un élément de G et y_1y_2 sa factorisation, on a $xy = x_1x_2y_1y_2$ qui, en vertu de 2), s'écrit aussi $x_1y_1x_2y_2$, d'où $\varphi(xy) = (x_1y_1, x_2y_2) = \varphi(x)\varphi(y)$.

En résumé : *Pour que le groupe* G, *produit de deux de ses sous-groupes g_1 et g_2, en soit le produit direct, il est nécessaire et suffisant que l'un des deux groupes de conditions (1 et 2) ou (3 et 4) soit satisfait.*

En particulier, si G *est commutatif, il faut et il suffit que la condition 1* (unicité de la factorisation) *ou la condition équivalente (3)* ($g_1 \cap g_2 = \{e\}$) *soit satisfaite.*

Notations : Dans le cas où le groupe est noté additivement (auquel cas on parlera de somme directe), on notera :

$$G = g_1 \oplus g_2.$$

Mais en cas de notation multiplicative, il ne faut pas utiliser $\otimes$ réservé à un autre usage.

Insistons encore sur le fait qu'un groupe G qui admet un sous-groupe invariant g_1 n'est pas nécessairement pour cela isomorphe au produit cartésien $G/g_1 \times g_1$, même dans le cas où G/g_1 est isomorphe à un autre sous-groupe invariant g_2. Nous verrons à ce sujet l'exercice 29.

Exemples : En attendant, donnons différents exemples de diverses circonstances possibles.

Un exemple de la dernière circonstance signalée nous est fourni par le groupe $\mathbf{Z}_8$ des entiers additifs modulo 8. Ce groupe admet le sous-groupe invariant $g_1 = \{0, 2, 4, 6\}$ et $\mathbf{Z}_8/g_1$ est d'ordre 2. Or, $\mathbf{Z}_8$ possède aussi un sous-groupe d'ordre 2 : $g_2 = \{0, 4\}$, nécessairement isomorphe à $\mathbf{Z}_8/g_1$, mais $\mathbf{Z}_8$ n'est pas somme directe (et ici n'est pas somme non plus au sens des opérations sur les parties) de g_1 et g_2.

Dans **Z**, nous avons déjà montré (II, 3, 1) qu'un groupe quotient de **Z** ne pouvait jamais être isomorphe à un sous-groupe et que **Z** ne pourrait donc jamais être non trivialement somme directe. En reprenant en quelque sorte la question à l'envers, nous pouvons choisir deux sous-groupes g_1 et g_2 tels que $\mathbf{Z} = g_1 + g_2$. On sait en effet que tous les sous-groupes de **Z** sont de la forme $m\mathbf{Z}$ (ensemble des multiples de m). Il suffira de choisir $g_1 = m\mathbf{Z}$ et $g_2 = n\mathbf{Z}$ avec m et n premiers entre eux pour que $\lambda m + \mu n$, somme d'un élément de g_1 et d'un élément de g_2, décrive tout **Z** comme on le démontre en arithmétique.

Mais $\mathbf{Z} \neq g_1 \oplus g_2$, car $g_1 \cap g_2 \neq \{e\}$ (ou, si l'on préfère, la mise d'un entier sous forme $\lambda m + \mu n$ est possible d'une infinité de façons).

Les deux *groupes d'ordre 4* (voir corrigé exercice 19) admettent l'un et l'autre le sous-groupe $\{e, a\}$ de table de groupe

	e	a
e	e	a
a	a	e

et le groupe quotient $G/g_1 = \{g_1, bg_1\}$ de table de groupe :

	g_1	bg_1
g_1	g_1	bg_1
bg_1	bg_1	g_1

isomorphe à $g_2 = \{ e, b \}$ de table de groupe :

	e	b
e	e	b
b	b	e

Or, le produit $g_1 \times g_2$ a pour table (dont on n'écrit qu'une moitié en profitant de la commutativité) :

	(e, e)	(a, e)	(e, b)	(a, b)
(e, e)	(e, e)	(a, e)	(e, b)	(a, b)
(a, e)		(e, e)	(a, b)	(e, b)
(e, b)			(e, e)	(a, e)
(a, b)				(e, e)

isomorphe à :

	e	a	b	c
e	e	a	b	c
a		e	c	b
b			e	a
c				e

Le premier des groupes d'ordre 4 trouvés (celui des symétries par rapport aux 3 axes d'un trièdre trirectangle) apparaît donc comme le produit direct de deux de ses sous-groupes. Le deuxième, au contraire, ne l'est pas et n'a d'ailleurs même pas de sous-groupe isomorphe à G/g_1 (contrairement à ce qui se passait pour $\mathbf{Z}_8$).

Exercice 28. — Soient G_1 et G_2, deux groupes ayant respectivement deux sous-groupes invariants g_1 et g_2. Montrer que $G_1 \times G_2$ possède un sous-groupe invariant isomorphe à $g_1 \times g_2$ et que

$$G_1 \times G_2/g_1 \times g_2 \approx G_1/g_1 \times G_2/g_1$$

Exemple : Un tore T_2 peut être considéré comme produit cartésien $T_1 \times T_1$. On peut aussi dans $\mathbf{R}^2$ considérer le sous-groupe $\mathbf{Z}^2$ et le tore T_2 comme le quotient $\mathbf{R}^2/\mathbf{Z}^2$.

Exercice 29. — Une condition nécessaire et suffisante pour que, H étant un sous-groupe invariant de G on ait $G \approx H \times G/H$, est qu'il existe un homomorphisme de G sur H dont la restriction à H soit l'identité (c'est-à-dire $f(x) \approx x$ pour tout x).

Exercice 30. — Si G est commutatif et H un de ses sous-groupes, si G/H est monogène infini montrer que

$$G \approx H \times G/H.$$

§ 4. GROUPES ORDONNES

1. On appelle groupe ordonné un ensemble G muni d'une structure d'ordre et d'une structure de groupe compatibles entre elles, c'est-à-dire que :

$$\forall x \in G \qquad a \prec b \Rightarrow \begin{cases} ax \prec bx \\ xa \prec xb \end{cases}$$

Remarquons d'abord que les formules d'antériorité peuvent être multipliées membre à membre :

$$\left.\begin{matrix} a \prec b \\ c \prec d \end{matrix}\right\} \Rightarrow \left.\begin{matrix} ac \prec bc \\ bc \prec bd \end{matrix}\right\} \Rightarrow ac \prec bd$$

Remarquons ensuite que

$$a \prec b \Rightarrow \begin{cases} a\,b^{-1} \prec e \prec a^{-1}\,b \\ b^{-1}\,a \prec e \prec b\,a^{-1} \end{cases}$$

et qu'une seule des 4 formules de droite implique celle de gauche. Il en résulte que la structure d'ordre sur G est donnée par la connaissance des éléments postérieurs à e dont l'ensemble est désigné par G^+.

Exemple : groupe additif du plan. Le plan $\mathbf{R}^2$ est un groupe (v. p. 45) ordonné (voir page 23). S'il est ordonné par la relation :

$$(x, y) \prec (x', y') \Longleftrightarrow x \prec x', y \prec y',\ G^+ \text{ est le } 1^{er} \text{ quadrant.}$$

S'il est ordonné par l'ordre lexicographique, G^+ est constitué par l'ensemble des quadrants I et IV et de la partie positive de l'axe des ordonnées ($x > 0$, y quelconque ; $x = 0$, $y \geqslant 0$).

Propriétés de G^+ : $e \prec a$, $e \prec b \Rightarrow e \prec ab$, donc $(G^+)^2 \subset G^+$, mais $G^+ \subset (G^+)^2$ (il suffit de considérer les produits ea où a décrit G^+ pour voir que G^+ est une partie de $(G^+)^2$). Donc :

$$(G^+)^2 = G^+, \tag{1}$$

G^+ est invariant dans tous les automorphismes intérieurs de G, car

$$e \prec b \Rightarrow a\,e\,a^{-1} \prec a\,b\,a^{-1}, \text{ soit } e \prec aba^{-1}$$

$$aG^+a^{-1} = G^+. \tag{2}$$

D'autre part, si $e \prec a$ $\quad a^{-1} \prec e$

et si $e \succ a$ $\quad a^{-1} \succ e$

Posons $G^- = (G^+)^{-1}$; on vient donc de constater que

$$G^+ \cap G^- = \{ e \}. \tag{3}$$

Les propriétés de G^+ que nous venons d'établir sont caractéristiques du sous-ensemble G^+ d'un groupe ordonné ; c'est-à-dire que l'on peut définir sur le groupe G, admettant un tel sous-ensemble, une relation d'ordre telle que G^+ soit l'ensemble des éléments $\succ e$. Soit donc : $G^+ \subset G$ tel que $(G^+)^2 = G^+$; $\forall a \in G$, $a\,G^+\,a^{-1} = G^+$; $G^+ \cap G^- = \{ e \}$. (Sur un groupe commutatif, la 2e des 3 conditions disparaît).

Soit la relation

$$a \prec b \Longleftrightarrow ba^{-1} \in G^+,$$

montrons que c'est une relation d'ordre :

1) elle est réflexive car $\forall a \quad aa^{-1} = e \in G^+$;

2) elle est antisymétrique car $\forall (a, b) \in G^2$,
$ab^{-1} \in G^+$, $ba^{-1} \in G^+ \Rightarrow (ba^{-1})^{-1} = a\,b^{-1} \in G^-$ donc $a\,b^{-1} = e$;

3) elle est transitive car $\forall (a, b, c) \in G^3$,
$ba^{-1} \in G^+$, $cb^{-1} \in G^+ \Rightarrow cb^{-1}ba^{-1} = ca^{-1} \in G^+$,
puisque $(G^+)^2 = G^+$.

Reste à vérifier la compatibilité avec la loi de groupe. Soient a et b tels que : $ba^{-1} \in G^+$.

Formons $\quad bx\,(ax)^{-1} = bx\,x^{-1}\,a^{-1} = ba^{-1} \in G^+$

et $\quad xb\,(xa)^{-1} = xba^{-1}x^{-1}$,

$ba^{-1} \in G^+$ et l'invariance de G^+ dans les automorphismes intérieurs montre que $xba^{-1}x^{-1}$ appartient aussi à G^+,

donc :

$$a \prec b \Rightarrow \begin{cases} ax \prec bx \\ xa \prec xb. \end{cases}$$

Nous sommes maintenant en mesure de chercher toutes les structures d'ordre dont on peut doter un groupe G en cherchant tous les sous-ensembles G+ possibles.

Exemples : Dans le groupe additif $\mathbf{R}^2$ on peut prendre pour G+ un secteur convexe (angle saillant) de sommet O. G− étant le secteur symétrique par rapport à O, $G^+ \cap G^- = \{ O \}$ et la première condition est aussi vérifiée. (L'ensemble des points à coordonnées entières $\geqslant 0$ peut aussi être pris pour G+).

Sur $\mathbf{Q}^+$, ensemble des rationnels positifs considéré comme groupe par rapport à la multiplication, on pourra prendre pour $(\mathbf{Q}^+)^+$ l'ensemble des entiers naturels, $a \prec b$ veut alors dire b/a entier, c'est-à-dire si a et b sont entiers : $a|b$.

2. Groupes réticulés.

C'est un groupe ordonné qui, pour son ordre, est un treillis, c'est-à-dire qui est tel que, pour tout couple (a, b) on puisse définir $a \mathbf{V} b$ et $a \mathbf{\Lambda} b$.

Tous les exemples de groupes ordonnés que nous venons de citer étaient réticulés.

Nous nous bornerons à étudier les propriétés de ces groupes dans le cas où ils sont *commutatifs* et nous utiliserons une notation additive.

Première propriété. $\quad a + b \mathbf{V} c = (a + b) \mathbf{V} (a + c)$.

En effet,

$$\left.\begin{matrix} b \prec b \mathbf{V} c \\ c \prec b \mathbf{V} c \end{matrix}\right\} \text{ entraînent grâce à la compatibilité avec la loi de groupe :}$$

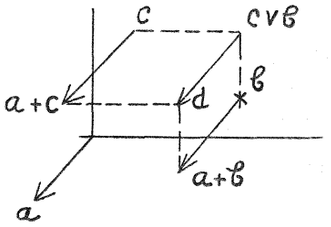
$$\left.\begin{matrix} a + c \prec a + b \mathbf{V} c \\ a + b \prec a + b \mathbf{V} c \end{matrix}\right\} \Rightarrow (a + b) \mathbf{V} (a + c) \prec a + b \mathbf{V} c \quad (1).$$

Mais appliquons cette règle à $(a + b) \mathbf{V} (a + c)$ en prenant comme élément à ajouter $(-a)$. Il vient :

$$b \mathbf{V} c \prec (a + b) \mathbf{V} (a + c) + (-a),$$

donc $\quad a + b \mathbf{V} c \prec (a + b) \mathbf{V} (a + c)$,

ce qui, rapproché de l'égalité (1), démontre l'égalité indiquée qui peut s'exprimer : si on ajoute un même élément aux deux éléments d'un couple, leur sup est augmenté du même élément.



$$d = (a + c) \ \mathbf{V} \ (a + b).$$

Remarquons qu'appliquée au groupe additif du plan (ordonné avec $G^+ = 1^{er}$ quadrant), cette égalité exprime simplement que la translation a laisse invariante la figure formée par b, c et leur sup. On démontre de même (en remplaçant partout $\prec$ par $\succ$ et $\mathbf{V}$ par $\mathbf{\Lambda}$) que

$$a + b \mathbf{\Lambda} c = (a + b) \mathbf{\Lambda} (a + c).$$

Deuxième propriété. $\quad b \mathbf{V} c + b \mathbf{\Lambda} c = b + c$.

Faisons $a = b \mathbf{V} c$ dans l'égalité précédemment établie :

$$b \mathbf{V} c + b \mathbf{\Lambda} c = (b \mathbf{V} c + b) \mathbf{\Lambda} (b \mathbf{V} c + c).$$

Mais $\quad b \mathbf{V} c + b = 2b \mathbf{V} (c + b) \succ b + c$,

$$b \mathbf{V} c + c = (c + b) \mathbf{V} 2c \succ b + c.$$

L'inf de ces deux éléments est donc aussi $\succ b + c$,

donc : $\quad b \mathbf{V} c + b \mathbf{\Lambda} c \succ b + c$.

Mais on montrerait de même (avec échange des $\prec$ et $\succ$, $\mathbf{V}$ et $\mathbf{\Lambda}$) que :

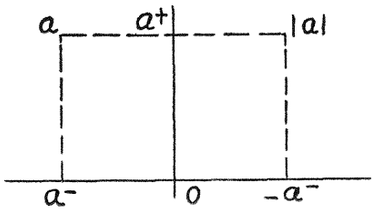
$$b \mathbf{\Lambda} c + b \mathbf{V} c \prec b + c.$$

Le rapprochement de ces deux formules démontre l'égalité indiquée. Remarquons qu'appliquée au groupe multiplicatif des rationnels (ordonné par la relation $a \prec b \Longleftrightarrow ba^{-1}$ entier) et à deux éléments entiers, cette dernière propriété n'est autre que :

P.P.C.M. $\times$ P.G.C.D. = produit des 2 nombres.

Quelques nouvelles définitions : 0 représentant l'élément neutre, on pose : $a^+ = a \mathbf{V} 0$ et $a^- = a \mathbf{\Lambda} 0$.

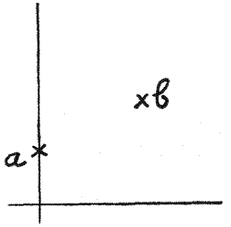
La règle précédente donne : $a^+ + a^- = a$ et on convient de poser $a^+ - a^- = |a|$ que l'on appelle *valeur absolue* de a. Ces diverses notations sont figurées sur le schéma ci-dessous dans le cas du groupe additif $\mathbf{R}^2$ et pour un élément qui n'appartient ni à G+ ni à G−.



Exercice 31. — Montrer que $|a + b| < |a| + |b|$ et que $|a - b| = a \mathbf{V} b - a \mathbf{\Lambda} b$.

3. Groupe archimédien.

On appelle archimédien un groupe ordonné où a étant un élément $\succ 0$ et $\neq 0$ et b donné, on ne peut avoir $na \prec b$ quel que soit $n \in \mathbf{N}$.



De nombreux groupes usuels sont archimédiens mais pas tous. Exemple : dans le plan ordonné par l'ordre lexicographique, on pourra avoir $na \prec b$ pour tout n (voir figure ci-dessus).

Exercice 32 *(sur les groupes réticulés).* — Soit G un groupe réticulé commutatif noté additivement.

1) Montrer que

$$\forall a \in G,\ b \in G \qquad -(a \vee b) = (-a) \wedge (-b)$$

2) On veut prouver qu'en tant que treillis G est distributif c'est-à-dire que $\forall (a, b, c) \in G^3$ on a

$$(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$$
$$(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$$

a) Montrer qu'il suffit d'établir une des deux égalités précédentes.

b) Montrer que dans tout treillis

$$(a \wedge b) \vee c \prec (a \vee c) \wedge (b \vee c)$$

c) Montrer que dans G

$$(a \wedge b) \vee c \succ (a \vee c) \wedge (b \vee c)$$

Pour cela on montrera :

α) qu'on peut se ramener au cas où $a \wedge b = 0$,

β) que si a est positif $a \vee c = a \vee c+$

et on déduira l'égalité cherchée.

3) Montrer que $n(a \wedge 0) = na \wedge (n-1)a \wedge \ldots \wedge a \wedge 0$, n entier > 0.

En déduire que $na \succ 0$ implique $a \succ 0$.

4) Montrer $a+ \wedge -(a-) = (a \wedge -a) \vee 0$

et en déduire que $a+ \wedge -(a-) = 0$.

Exercice 33. — Montrer que dans un groupe réticulé les deux égalités

$$a \vee x = a \vee y$$
$$a \wedge x = a \wedge y$$

impliquent $x = y$

§ 5. GROUPES DE TRANSFORMATION

E étant un ensemble, on considère l'ensemble des bijections de E sur E désigné par S_E. Cet ensemble constitue un groupe appelé *groupe symétrique de* E.

La loi de groupe est évidemment la composition et l'inverse d'une bijection f est la bijection réciproque, c'est-à-dire

$$f^{-1} = \overset{-1}{f}$$

Quand E est un ensemble fini de n éléments, le groupe symétrique des bijections de E sur E, appelé S_n, a n ! éléments.

Les transformations de la géométrie élémentaire sont des bijections (même la transformation par polaires réciproques à condition de considérer des ensembles d'éléments de contact), l'ensemble E étant, par exemple, le plan euclidien, le plan projectif ou le plan anallagmatique. Il n'y a pas de différence de nature entre un groupe de transformation et un groupe abstrait, car tout groupe peut être considéré comme un groupe de transformation.

Soit en effet la bijection $x \overset{(a)}{\longrightarrow} a\,x$

qui applique G sur lui-même. Le composé des bijections (a) et (b), soit $(b) \circ (a)$, fait correspondre à x l'élément $b\,a\,x$. Le groupe G est donc isomorphe à un sous-groupe de ses transformations sur lui-même (isomorphisme qui à $a \in G$ fait correspondre la bijection $(a) \in s_G \subset S_G$). En identifiant G et s_G on écrira :

$$G \subset S_G .$$

Supposons maintenant que soit donné un ensemble E et que G soit

homomorphe à un sous-groupe $s_E \subset S_E$, c'est-à-dire qu'à tout élément $\alpha \in G$ je puisse faire correspondre une bijection (α) de E sur lui-même. Cette bijection (α) envoie x sur un élément x' de E que nous noterons par αx. Nous avons ainsi défini sur E une loi de composition externe qui à tout α de G et à tout x de E fait correspondre $x' = \alpha x$, image de x par la bijection (α).

$$G \times E \longrightarrow E$$
$$(\alpha, x) \longrightarrow \alpha x.$$

Les éléments de G sont dits des opérateurs et on dit que G opère dans E. Remarquons que cette loi de composition externe n'est pas quelconque. En effet, faisons subir à x la bijection $(\beta) \circ (\alpha)$:

$$x \overset{(\alpha)}{\longrightarrow} \alpha x \overset{(\beta)}{\longrightarrow} \beta\,(\alpha x).$$

Mais l'homomorphisme entre G et le sous-groupe des bijections exige que

$$(\beta\alpha) = (\beta) \circ (\alpha).$$

Or, la bijection $\beta\alpha$ envoie x sur $\beta\alpha x$. La loi de composition externe précédemment définie satisfait donc à :

$$\beta\,(\alpha x) = \beta\alpha x.$$

D'autre part, la bijection (ε) correspondant à ε, élément neutre de G, est la bijection identique. Donc

$$\forall\, x \in E \qquad \varepsilon\, x = x.$$

Exercice 34. — Réciproquement si une opération externe est définie sur E, ses opérateurs appartenant à un groupe G et si cette loi vérifie les deux propriétés

$$\forall\, (\alpha, \beta) \in G^2 \qquad \forall\, x \in E \qquad \beta(\alpha x) = \beta\alpha x$$
$$\text{et} \quad \forall\, x \in E \qquad \varepsilon x = x$$

montrer que G est homomorphe à un sous-groupe de S_E.

G *opérant sur* E *est transitif*, si

$$\forall\, (x, y) \in E^2 \qquad \exists\, \alpha \in G \qquad y = \alpha x,$$

ce qui veut dire que les bijections du groupe G peuvent faire se correspondre deux éléments quelconques de E. Les déplacements (et même les translations) forment pour le plan un groupe transitif. Il n'en serait pas de même pour les rotations de centre donné.

Si G n'est pas transitif, il est intéressant de savoir quels sont les couples x, y dont G peut faire correspondre les éléments. Posons

$$x R y \iff \exists\, \alpha \qquad y = \alpha x.$$

On vérifie que R est une relation d'équivalence. Dans une même classe on trouve tous les éléments qui peuvent être envoyés les uns sur les autres. (Pour les rotations de centre O, une classe d'équivalence est un cercle de centre O).

§ 6. PLONGEMENT D'UN DEMI-GROUPE ABELIEN DANS UN GROUPE ABELIEN

1. (Nous utiliserons, sauf indication contraire, la notation multiplicative).

Une propriété fondamentale des groupes est qu'il existe pour tout couple (a, b) un élément x et un seul tel que $ax = b$. Or, certains ensembles où une loi de composition est définie ne jouissent pas de cette propriété, certaines des équations $ax = b$ ne possédant pas de solution dans l'ensemble et il est naturel de chercher à plonger l'ensemble dans un

ensemble plus vaste tel que ces équations y possèdent alors toutes une solution.

De façon plus précise, étant donné l'ensemble D sur lequel est définie une loi de composition, il s'agit de trouver un groupe $G \supset D$ tel que la loi induite sur D par celle de G soit celle de D. Nous allons chercher à quelles conditions doit satisfaire D pour que cette opération soit possible.

Conditions nécessairement vérifiées par D.

Une première condition apparaît évidente : c'est que la loi sur D soit associative.

D'autre part, D doit être une partie stable de G pour l'opération de groupe de G. Et, a étant un élément de G, nous avons vu que l'application

$$\begin{array}{ccc} G & \longrightarrow & G \\ x & & ax \end{array}$$

était une bijection. Il faut donc que l'application

$$\begin{array}{ccccc} D & \longrightarrow & D & & \\ x & & ax & & a \in D \end{array}$$

soit la restriction à D d'une application bijective. Or, cette restriction n'a aucune raison d'être surjective, mais elle doit être injective ; on doit pouvoir affirmer :

$$ax = ay \Rightarrow x = y,$$

ce qui peut encore s'exprimer : dans D, une égalité doit être simplifiable.

Nous voyons donc qu'on doit imposer à D que sa loi de composition soit *associative* et que les égalités y soient *simplifiables*. Et nous allons montrer que si nous ajoutons à ces conditions celle que G soit commutatif, ce qui entraîne que la loi de composition sur D soit *commutative*, le problème de construction de G admet une solution et une seule.

Construction de G. Nous la ferons en partant de deux idées voisines qui nous conduiront au même résultat.

Premier point de vue : Pour transformer D en un groupe, il est d'abord nécessaire de lui adjoindre un élément neutre s'il n'en possédait pas. Il faut ensuite lui ajouter les inverses de ceux des éléments de D qui n'en ont pas. Pour que G soit un groupe, il devra enfin contenir tous les éléments de la forme xy^{-1} et leurs produits.

[Les mots « inverse » et « produit » sont pris ici dans leur sens relatif à la loi de composition à déterminer pour G, détermination qui fait partie de la construction de G].

Observons tout de suite que le produit de deux éléments de la forme xy^{-1} est lui aussi de cette forme, c'est-à-dire que leur ensemble est fermé pour la loi de composition ; en effet,

$$xy^{-1}\, uv^{-1} = xuy^{-1}v^{-1}$$

grâce à l'hypothèse de commutativité ; et

$$xuy^{-1}v^{-1} = xu\,(yv)^{-1}.$$

Mais certains éléments de cette nature peuvent être égaux :

$$xy^{-1} = uv^{-1} \text{ si } xv = yu \quad (1).$$

La loi de composition qui intervient dans cette égalité étant cette fois la loi induite sur D, donc la loi connue.

Or, nous constatons que la relation R définie par

$$(x, y)\ \mathrm{R}\ (u, v) \Longleftrightarrow xv = yu$$

est réflexive, symétrique (ce qui est immédiat) et transitive, car

$$(x, y)\ \mathrm{R}\ (u, v) \Longleftrightarrow xv = yu$$
$$(u, v)\ \mathrm{R}\ (s, t) \Longleftrightarrow ut = vs,$$

en multipliant la première égalité par t, la deuxième par y, il vient :

$$xvt = vsy \Rightarrow xt = sy \Rightarrow (x, y)\ \mathrm{R}\ (s, t),$$

en utilisant le fait que les égalités sont simplifiables. R détermine donc une partition sur l'ensemble des couples d'éléments de D ; en d'autres termes, un élément de G correspond à un élément de D^2/R.

Deuxième point de vue : Considérons les équations $ax = b$, a et b appartenant à D. Si elles ont une solution, c'est qu'au couple $(a, b) \in D^2$ on peut faire correspondre $x \in D$, parfaitement défini par $ax = b$. (Le fait que les égalités sont simplifiables exclut la possibilité de deux solutions distinctes d'une telle équation). Mais cette correspondance n'est pas injective car

$$ax = b \Rightarrow amx = bm,$$

et les couples (a, b) et $(c = am, d = bm)$ ont la même image x dans cette correspondance. Deux tels couples vérifient $ad = bc$ et réciproquement tout couple (c, d) tel que $ad = bc$ aura la même image x que (a, b) car

$$ax = b \Rightarrow acx = bc = ad \Rightarrow cx = d.$$

Tout x, solution d'une équation $ax = b$, correspond donc à une famille d'éléments de D^2 ou à un élément de D^2/R, R ayant la même signification que précédemment.

L'idée est alors de manipuler les couples (a, b) pour lesquels il n'y avait pas de solution dans D, comme s'il y en avait une. Nous nous trouvons amenés à nouveau à considérer l'ensemble D^2/R.

Mais D n'est pas un sous-ensemble de D^2/R puisque leurs éléments ne sont pas de même nature. Il y a seulement correspondance entre les éléments de D et certains éléments de D^2/R. Ceci nous amène à modifier légèrement l'énoncé du problème posé :

On dira qu'on plonge un ensemble D muni d'une loi de composition dans un groupe G si on peut déterminer ce groupe G de telle façon qu'il possède un sous-ensemble qui, pour la loi de composition de G, soit isomorphe à D.

Les deux raisonnements faits précédemment ont montré qu'un ensemble G répondant à la question ainsi posée devait nécessairement contenir D^2/R (ou un ensemble isomorphe à D^2/R). Si nous montrons maintenant que D^2/R y satisfait effectivement, nous aurons montré que les conditions imposées à D étaient suffisantes et que D^2/R est le plus petit groupe répondant à la question (déterminé à un isomorphisme près).

La loi de composition sur D^2/R est évidemment définie par la loi de composition sur D^2 appliquée aux éléments de chacune des classes.

$$\dot{\overline{(a, b)}}\ \dot{\overline{(c, d)}} = \dot{\overline{(ac, bd)}},$$

ce qui n'a de sens que si le résultat est indépendant du couple d'éléments choisi dans une classe. Vérifions-le : soit

$$(a', b') \in \dot{\overline{(a, b)}}, \text{ c'est-à-dire tel que } ab' = ba'$$

et formons $(a'c, b'd)$. Il appartient bien à $\dot{\overline{(ac, bd)}}$, car

$$acb'd = bda'c.$$

Cette loi de composition donne à D^2/R une structure de groupe. En effet :

1) elle est associative ;

2) elle possède un élément neutre $\dot{\overline{(a, a)}}$, car

$$\dot{\overline{(u, v)}}\ \dot{\overline{(a, a)}} = \dot{\overline{(ua, va)}} = \dot{\overline{(u, v)}} ;$$

3) tout élément (a, b) a un inverse (b, a), car

$$\dot{\overline{(a, b)}}\ \dot{\overline{(b, a)}} = \dot{\overline{(ab, ab)}}.$$

Reste à voir si D^2/R contient un sous-ensemble qui soit isomorphe à D. Nous appellerons ce sous-ensemble $\widehat{D}$; nous allons voir qu'il est constitué par l'ensemble des classes $\dot{\overline{(ab, b)}}$. En effet, faisons correspondre à tout $a \in D$ la classe $\dot{\overline{(ab, b)}}$.

$$D \longrightarrow D^2/R$$
$$a \qquad \dot{\overline{(ab, b)}}.$$

Cette application est un homomorphisme car elle fait correspondre :

$$a_1 \longrightarrow \dot{\overline{(a_1b_1, b_1)}}$$
$$a_2 \longrightarrow \dot{\overline{(a_2b_2, b_2)}}$$
$$a_1a_2 \longrightarrow \dot{\overline{(a_1a_2b_3, b_3)}}.$$

Mais le produit des 2 classes images de a_1 et a_2 est :

$$\dot{\overline{(a_1b_1a_2b_2, b_1b_2)}} = \dot{\overline{(a_1a_2b_1b_2, b_1b_2)}}.$$

Cet homomorphisme est injectif car

$$\dot{\overline{(a_1b_1, b_1)}} = \dot{\overline{(a_2b_2, b_2)}} \Rightarrow a_1b_1b_2 = b_1a_2b_2 \Rightarrow a_1 = a_2.$$

Si nous considérons alors l'application

$$D \longrightarrow \widehat{D}$$

qui, elle, sera surjective, nous voyons que nous avons affaire à une bijection et que

$$D \approx \widehat{D}.$$

On peut identifier alors D et $\widehat{D}$ si on veut donner une solution au problème tel que nous l'avions initialement formulé.

En résumé : Nous appellerons *demi-groupe commutatif un ensemble sur lequel est définie une opération associative, commutative et simplifiable.*

Et la conclusion de l'étude précédente s'énoncera : *Pour qu'un ensemble muni d'une loi de composition puisse être plongé dans un groupe commutatif, il faut et il suffit que ce soit un demi-groupe commutatif, et le plus petit groupe commutatif contenant le demi-groupe est alors déterminé de manière unique (à un isomorphisme près).*

Application à **N**. Considérons l'ensemble **N** des entiers naturels. **N** est muni de deux lois de composition associatives, commutatives et simplifiables. Il pourra donc être considéré comme demi-groupe pour chacune et, en conséquence, pourra être plongé dans un groupe additif et dans un groupe multiplicatif.

2. Construction de Z, groupe additif des entiers.

Les éléments de N^2/R sont des classes de couples d'entiers naturels ; (a, b) et (c, d) sont dans la même classe si $a + d = b + c$. L'ensemble $\widehat{N}$ est l'ensemble des classes $\dot{\overline{(a + b, b)}}$, c'est-à-dire celui des classes $\dot{\overline{(a, b)}}$ où $a \geqslant b$ (mettre $\geqslant$ est admettre que 0 fait partie des entiers naturels). Dans chacune de ces classes il existe un représentant remarquable $(c, 0)$ avec $c = a - b$. Si au contraire $a \leqslant b$, il existe dans la classe (a, b) le représentant $(0, c)$ avec $c = b - a$. L'habitude est de poser

$$(c, 0) = c \qquad \text{(Identification de } \widehat{N} \text{ et de N)}$$
et $$(0, c) = -c,$$

$(c, 0)$ et $(0, c)$, dont la somme est (c, c) qui appartient à la classe neutre, sont évidemment des éléments inverses.

Ordre sur **Z**. Sans se servir de l'ordre que possède **N**, on peut remarquer que pour l'ensemble **Z**, **N** a les propriétés d'un G^+. L'ensemble G^- est constitué par l'ensemble des classes $\dot{\overline{(0, c)}}$ et **Z** est alors formé de la réunion de **N** et N^-. Il en résulte que **Z** est muni d'une *structure d'ordre total* puisque, étant donnés deux éléments quelconques, le composé de l'un avec l'inverse (ici opposé) de l'autre appartient nécessairement soit à **N**, soit à N^-. L'ordre ainsi obtenu sur **Z** induit d'ailleurs sur **N** l'ordre naturel.

3. Construction de Q^+ (groupe multiplicatif des rationnels positifs).

La classe $\dot{\overline{(a, b)}}$ ne possède pas cette fois d'élément donnant une forme réduite aussi jolie. On peut toutefois, en divisant a et b par leur P.G.C.D., prendre comme représentant de la classe un couple dont les deux termes soient premiers entre eux (fraction réduite à sa plus simple expression). Contrairement à ce qui se passe pour **Z**, on a d'ailleurs l'habitude de travailler avec n'importe quel représentant des classes.

On peut encore prendre **N** comme G^+ de Q^+ (voir groupes ordonnés, exemple page 50), mais $N \cup N^- \neq Q^+$ (N^- n'a évidemment pas la même signification que dans le paragraphe précédent) et l'ordre ainsi établi sur Q^+ n'est pas total.

CHAPITRE III

ANNEAUX - CORPS

§ 1. PRINCIPALES STRUCTURES ALGEBRIQUES

Avant d'aborder l'étude de ces deux structures, nous donnons la liste des principales structures algébriques :

1. Anneau (Ring en anglais et en allemand).

C'est un ensemble muni de deux lois de composition :

La 1re (notée additivement) est une loi de groupe commutatif.

La 2e (notée multiplicativement) est associative et distributive par rapport à la 1re.

$$\forall a, b, c \begin{cases} (a+b)\,c = ac + bc \\ c\,(a+b) = ca + cb. \end{cases}$$

Si la 2e loi est commutative, on dit que l'anneau est commutatif.

S'il existe un élément neutre pour la 2e loi, l'anneau est dit « à élément unité » ou « unitaire », et cet élément neutre est appelé unité.

Dans un anneau on a, si 0 est l'élément neutre de la 1re loi :

$$ba = (b+0)\,a = ba + 0a \quad \text{et} \quad ab = a\,(b+0) = ab + a0.$$

Donc $\forall a \qquad 0a = a0 = 0.$

Exemple d'anneau : **Z** (voir exercice 35).

2. Corps (field en anglais, Körper en allemand).

1) Un corps K est d'abord un anneau.

2) Si on retire de K l'élément neutre de la première opération, l'ensemble obtenu $K - \{0\} = K^*$ est un groupe pour la 2e opération.

Un corps peut être commutatif ou non commutatif. Dans ce cas, il est dit « gauche » (skew field ou sfield en anglais).

Exemples de corps :

Q corps des rationnels
R corps des réels
C corps des complexes.

Exercice 35 *(définition des opérations sur* **Z** *et sur* **Q** *à partir des opérations de* **N**. *Structure d'anneau sur* **Z** *et de corps sur* **Q**).

1) On a obtenu plus haut **Z** comme plus petit groupe commutatif contenant **N** (l'opération de **Z** induisant l'addition sur **N**).

Montrer qu'il existe une opération et une seule sur $\mathbf{Z}$, possédant les deux propriétés :

a) être distributive par rapport à l'addition,

b) induire sur $\mathbf{N}$ la multiplication,

et retrouver ses propriétés classiques (commutativité, règle des signes, produit des valeurs absolues, absence de diviseurs de zéro, comportement à l'égard de l'ordre sur $\mathbf{Z}$).

2) On remarque que $\mathbf{Z} - \{0\}$ est un demi-groupe commutatif pour la multiplication. Q est la réunion de $\{0\}$ et du plus petit groupe commutatif contenant $\mathbf{Z} - \{0\}$ et dont l'opération induit la multiplication sur $\mathbf{Z} - \{0\}$.

Montrer qu'il existe un unique prolongement de la multiplication ainsi définie sur $\mathbf{Q} - \{0\}$ à $\mathbf{Q}$ tout entier et une opération et une seule sur $\mathbf{Q}$ possédant les deux propriétés :

a) la multiplication est distributive par rapport à elle,

b) elle induit l'addition sur $\mathbf{Z}$,

et retrouver les propriétés de cette opération.

3. Espace vectoriel (linear space ou vector space en anglais, Vektorraum en allemand).

On se donne un ensemble E et un corps K ; nous nous bornerons ici au cas où ce corps K est commutatif et nous dirons que E est un espace vectoriel sur K si :

1) E a une structure de groupe commutatif (opération notée $+$) ;

2) il existe une opération externe $\underset{(x,\lambda)}{E \times K} \to \underset{\lambda x}{E}$

satisfaisant aux conditions suivantes : $\lambda(\mu x) = \lambda \mu x$

$$\lambda(x + y) = \lambda x + \lambda y$$
$$(\lambda + \mu) x = \lambda x + \mu x$$
$$1x = x.$$

On retrouve dans ces axiomes de la structure d'espace vectoriel les propriétés signalées pour les groupes d'opérateurs sur un espace E, propriétés auxquelles on a ajouté la double propriété de distributivité par rapport à la somme sur K et à la somme sur E de l'opération externe.

Exercice 36. — Montrer que si l'on a tous les axiomes des espaces vectoriels sauf $1x = x$, E (groupe commutatif) est la somme directe de deux sous-groupes E_1 et E_2 tels que l'on ait

$$\forall x_1 \in E_1 \qquad 1x_1 = x_1$$
$$\forall x_2 \in E_2 \qquad 1x_2 = 0$$

E_1 a une structure d'espace vectoriel pour les opérations induites sur lui.

On montrerait de la même façon que dans les anneaux que

$$\lambda 0 = 0 \qquad \forall \lambda \in K$$
$$0x = 0 \qquad \forall x \in E.$$

Dans ces deux égalités, 0 ne représente pas le même élément (élément de E dans la première, élément de K dans la 2e). L'habitude est de ne pas les distinguer quand aucun ennui ne peut en résulter.

Exemples d'espace vectoriel : Le plan $\mathbf{R}^2$ ou l'espace $\mathbf{R}^3$ (munis de leurs structures de groupe additif) sur le corps des réels. Tout corps peut aussi être considéré comme espace vectoriel sur lui-même.

4. Module.

La définition d'un module ne diffère de celle d'un espace vectoriel que sur un point : les opérateurs λ n'appartiennent plus à un corps K mais à un anneau. Nous nous bornerons encore au cas où cet anneau sera commutatif.

Exemple de module : Tout groupe abélien G est un module sur $\mathbf{Z}$ (on dit aussi un Z-module), l'opération externe $n\,a$ pour $n \in \mathbf{Z}$, $a \in G$ étant définie par :

$$\underbrace{n\,a = a + a + \ldots\ldots\ldots + a}_{n \text{ termes}} \quad \text{si } n > 0$$

$$\underbrace{n\,a = (-a) + (-a) + \ldots\ldots\ldots + (-a)}_{-n \text{ termes}} \quad \text{si } n < 0$$

L'étude des espaces vectoriels et des modules constitue l'*algèbre linéaire.*

5. Algèbre sur un corps (ou sur un anneau).

Soit K un corps (ou un anneau) commutatif et un ensemble E possédant une structure d'anneau. Cet anneau est une algèbre sur K si une loi de composition externe

$$\underset{(\lambda, x)}{K \times E} \longrightarrow \underset{\lambda x}{E}$$

est définie qui vérifie tous les axiomes de la structure d'espace vectoriel (ou de module) et vérifie en outre :

$$(\lambda x) y = \lambda(xy)$$
$$x(\lambda y) = \lambda(xy).$$

Exemple d'algèbre : L'ensemble des polynômes à une variable x à coefficients dans $\mathbf{R}$, ensemble que l'on notera $\mathbf{R}[x]$, est une algèbre sur $\mathbf{R}$. C'est en effet un anneau et la multiplication par un nombre réel satisfait à tous les axiomes posés.

Exercice 37. — On veut montrer que les structures d'un ensemble H permettent de définir des structures analogues sur l'ensemble $\mathcal{F}$ (E, H) des applications f de E dans H, E étant un ensemble dont on ne suppose rien.

On montrera en particulier :

1) que si H possède une loi de composition interne on peut en définir une sur $\mathcal{F}$ telle qu'en particulier si H est un groupe, $\mathcal{F}$ est un groupe dont H est d'une infinité de manières image homomorphe (indiquer quels sont les noyaux de ces homomorphismes) ; telle que, si H est un anneau $\mathcal{F}$ est un anneau ; mais telle que si H est un corps, $\mathcal{F}$ n'en est pas un si E a plus d'un élément ;

2) que si H possède une loi de composition externe on peut également doter $\mathcal{F}$ d'une loi de composition externe, l'ensemble des opérateurs étant le même et telle qu'en particulier si H est espace vectoriel sur un corps K, $\mathcal{F}$ est aussi espace vectoriel sur K ;

3) que si H possède une structure d'ordre (partiel ou total), $\mathcal{F}$ pourra être doté d'une structure d'ordre qui sera toujours partiel, si E a plus d'un élément ; que si H est un treillis, $\mathcal{F}$ en sera un aussi ;

4) que si une relation d'équivalence R est définie sur H, il en résulte une partition de $\mathcal{F}$. Que peut-on dire de l'ensemble des applications de E sur H/R ?

6. Homomorphisme de structures algébriques.

Nous dirons que deux ensembles E et F sont munis de structures homologues s'ils possèdent le même nombre de lois de composition interne et de lois de composition externe et s'il existe une correspondance bijective entre les lois de E et celles de F telle que chaque loi sur F jouisse des mêmes propriétés que son homologue sur E (commutativité, associativité, existence d'élément neutre, existence d'inverses...), que les propriétés des lois les unes par rapport aux autres (distributivité) se retrouvent sur leurs homologues.

E et F étant deux ensembles munis de structures homologues, une application f de E dans F sera un homomorphisme pour ces structures si elle en respecte toutes les opérations, c'est-à-dire si

$$f(x * y) = f(x) * f(y), \qquad (1).$$

pour toute loi $*$ définie sur E et son homologue dans F (notée de la même façon). Si la structure comprend des opérations externes, l'ensemble des opérateurs λ étant le même pour E et F, il faudra que :

$$f(\lambda x) = \lambda f(x). \qquad (2).$$

Si les ensembles d'opérateurs sont différents, il faudra qu'il existe une application φ de l'un de ces ensembles dans l'autre qui soit elle-même un homomorphisme pour leur structure et telle que :

$$f(\lambda x) = \varphi(\lambda) f(x). \qquad (2^{bis}).$$

Remarquons maintenant que, dans la définition de l'homomorphisme, l'hypothèse que les structures étaient homologues n'est pas intervenue, mais seulement l'existence du même nombre d'opérations sur E et F, et considérons un homomorphisme d'un ensemble E dans un ensemble F muni du même nombre d'opérations. Nous pouvons énoncer le résultat général suivant :

Si un ensemble E *possède une structure comportant un certain nombre de lois de composition et si f est un homomorphisme de* E *dans un ensemble* F *muni du même nombre de lois de composition,* f(E) *est une partie stable de* F *pour toutes les lois de composition sur* F *et a une structure homologue de celle de* F.

En effet, le fait que f(E) soit une partie stable de F résulte immédiatement des égalités (1). Ces égalités entraînent aussi le fait que si $*$ sur E est associative (resp. commutative), $*$ sur F sera associative (resp. commutative), que si E a un élément neutre e pour $*$, $f(e)$ est élément neutre dans f(E), et ainsi de suite.

Les égalités telles que (1) appliquées à deux lois différentes entraînent aussi que si l'une est distributive par rapport à l'autre dans E, les homologues le sont dans f(E) ; en effet :

$$x * (y \mathbf{T} z) = (x * y) \mathbf{T} (x * z)$$

entraîne :

$$f(x) * f(y \mathbf{T} z) = f(x * y) \mathbf{T} f(x * z),$$

et ceci entraîne :

$$f(x) * [f(y) \mathbf{T} f(z)] = [f(x) * f(y)] \mathbf{T} [f(x) * f(z)].$$

La dernière égalité exprime la distributivité annoncée. Enfin, les égalités (2) montrent que f(E) est aussi une partie stable pour une opération externe, et on vérifierait de façon analogue que les propriétés (distributivité..., etc...) de l'opération externe sur E se retrouvent sur f(E).

Nous pourrons donc dans l'ensemble F ne considérer que f(E). f sera alors un homomorphisme surjectif de E sur f(E). C'est dans ce cas que nous nous placerons dans ce qui suit immédiatement, même si nous notons par F l'ensemble d'arrivée.

Avant d'aller plus loin, nous ferons la remarque importante suivante :

Le composé de deux homomorphismes surjectifs est un homomorphisme surjectif. Soient f et g deux tels homomorphismes :

$$E \xrightarrow{f} F \xrightarrow{g} G.$$

L'application $g \circ f$ est un homomorphisme de E sur G comme on le vérifie immédiatement.

Factorisation des homomorphismes. Nous allons maintenant généraliser ce que nous avons fait pour les groupes et factoriser les homomorphismes de structures quelconques.

Soit donc :

$$E \xrightarrow{f} F$$

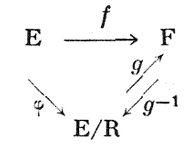
un homomorphisme surjectif et considérons sur E la relation :

$$x \mathrm{R} y \iff f(x) = f(y).$$

R est une relation d'équivalence sur E ; on peut donc considérer l'ensemble quotient E/R et, comme on l'a fait pour les groupes, l'application :

$$E/R \xrightarrow{g} F,$$

qui est bijective, donc permet d'attribuer à E/R une structure isomorphe de celle de F. Faisons alors le schéma suivant :



L'application φ : E $\longrightarrow$ E/R, peut être considérée comme le composé de f et de l'application g^{-1} : F $\longrightarrow$ E/R, qui est un isomorphisme. Il résulte alors de la remarque faite ci-dessus que :

$$\varphi = g^{-1} \circ f,$$

produit d'un homomorphisme par un isomorphisme est un homomorphisme.

On peut alors considérer que dans la décomposition $f = g \circ \varphi$, φ est un homomorphisme et g un isomorphisme :

$$E \xrightarrow{\varphi} E/R \xrightarrow{g} F$$

homomorphisme surjectif isomorphisme

Tout homomorphisme d'une structure sur une structure homologue peut être factorisé en un homomorphisme sur un espace quotient muni d'une structure homologue suivi d'un isomorphisme.

Ce qui va différer suivant les structures, c'est la signification de la relation R. Rappelons que si E était un groupe, celle-ci était de la forme :

$$x \mathrm{R} y \iff xy^{-1} \in g$$

g étant le sous-groupe invariant de $f(0)$.

Nous allons dans la suite chercher à préciser cette relation pour les principales structures et d'abord pour celle d'anneau.

§ 2. QUELQUES ANNEAUX IMPORTANTS

Nous avons déjà cité **Z**, 2**Z** (ensemble des entiers pairs), ou plus généralement $m\mathbf{Z}$. Notons que ces derniers ne possèdent pas d'élément unité.

1. Anneaux de polynômes.

Un autre exemple est l'anneau noté $A[x]$ des polynômes formels à une indéterminée à coefficients dans un anneau A. Un tel polynôme est une suite finie $[a_0, a_1, ..., a_n]$ d'éléments de A appelés coefficients du polynôme, ou, ce qui est équivalent, mais plus commode pour la définition des opérations, une suite infinie dont les termes sont nuls à partir d'un certain rang : $[a_0, a_1, ..., a_n, ...]$. Etant donnés deux polynômes $[a_0, a_1, ...]$ et $[b_0, b_1, ...]$ la somme est le polynôme $[a_0 + b_0, a_1 + b_1, ...]$ et le produit le polynôme $[c_0, c_1, ...]$ avec

$$c_q = a_0 b_q + a_1 b_{q-1} + ... + a_{q-1} b_1 + a_q b_0.$$

On vérifie aisément que ces opérations donnent à $A[x]$ une structure d'anneau (l'élément neutre de la 1re opération étant le polynôme dont tous les coefficients sont nuls). Si A a un élément unité 1, le polynôme $[1, 0, 0, ...]$ est élément unité de $A[x]$. Dans ce cas, en posant $x = [0, 1, 0, ...]$, on vérifie sans peine que

$$[a_0, a_1, ..., a_n, 0, ...] = a_0 + a_1 x + ... + a_n x^n.$$

La même notation sera souvent employée pour désigner le polynôme $[a_0, ..., a_n, 0, ...]$, même lorsque A n'est pas unitaire, mais alors x ne représente aucun élément de $A[x]$.

Le point de vue formel où l'on s'est placé diffère de celui de l'algèbre élémentaire où, d'une part, on prend pour A le corps **R**, et où, d'autre part, on considère que le polynôme P de coefficients $a_0, a_1, ..., a_n$ est l'application de **R** dans **R** qui à $\xi \in \mathbf{R}$ fait correspondre :

$$P(\xi) = a_0 + a_1 \xi + ... + a_n \xi^n.$$

L'ensemble $\mathcal{P}$ de ces polynômes-applications a une structure naturelle d'anneau (les opérations étant définies comme dans l'exercice 37). En faisant correspondre au polynôme formel $[a_0, ..., a_n] \in \mathbf{R}[x]$ le polynôme-application $\xi \to a_0 + a_1 \xi + ... + a_n \xi^n$ on définit un homomorphisme d'anneau de $\mathbf{R}[x]$ sur $\mathcal{P}$. C'est même ici un isomorphisme, en vertu du théorème classique : « deux polynômes-applications sont égaux si et seulement si leurs coefficients de même rang sont égaux », ou encore : « deux polynômes équivalents (égalité dans $\mathcal{P}$) sont identiques (égalité dans $\mathbf{R}[x]$) ». Ce théorème reste valable si on remplace **R** par un autre corps *infini*.

Mais on peut considérer une situation plus générale : si E est une algèbre unitaire sur l'anneau A, à tout polynôme $[a_0, ..., a_n] \in A[x]$ on peut faire correspondre l'application de A dans E qui à $\xi \in E$ fait correspondre $a_0 + a_1 \xi + ... + a_n \xi^n \in E$. L'ensemble $\mathcal{P}$ de ces applications a encore une structure naturelle d'anneau et on a encore un homomorphisme de $A[x]$ sur $\mathcal{P}$, mais ce n'est plus en général un isomorphisme. Prenons par exemple pour A et E le corps $\mathbf{Z}_2$ des entiers modulo 2. Aux deux polynômes formels 0 et $[0, 1, 1] = x + x^2$ correspond la même application de E dans E, car $0 + 0 = 1 + 1 = 0$.

On peut aussi considérer de la même façon des suites infinies de coefficients et les composer de la même façon. On obtiendra *l'anneau des séries formelles* à coefficients dans un anneau.

2. Diviseurs de zéro. Anneaux d'intégrité.

Nous savons que dans un anneau A :

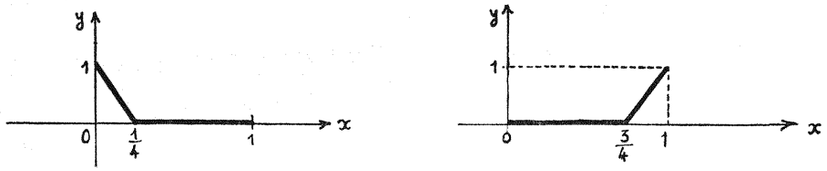
$$\forall x \in A. \qquad x0 = 0x = 0$$

On peut se demander si, réciproquement, de la nullité du produit, on peut conclure à celle d'un des facteurs du produit ou si, au contraire, le produit de deux éléments peut être nul sans que l'un d'entre eux le soit ; en d'autres termes si, dans l'anneau, existe des *diviseurs de zéro*. On appelle ainsi un élément a de l'anneau tel que :

$$a \neq 0 \qquad \exists b \in A \quad b \neq 0 \quad ab = 0 \text{ ou } ba = 0.$$

L'existence ou la non existence de diviseurs de zéro est une caractéristique importante des anneaux. Quand un anneau ne possède pas de diviseurs de zéro, on dit que c'est un *anneau d'intégrité* ou *anneau intègre*.

Il est facile de donner des exemples d'anneaux qui ne soient pas des anneaux d'intégrité : $\mathbf{Z}_6$ où $\dot{2} \times \dot{3} = \dot{0}$, et plus généralement tous les anneaux d'entiers modulo un nombre qui n'est pas premier ; ou bien l'ensemble des fonctions continues sur $[0, 1]$; sur l'anneau que forment ces fonctions, deux fonctions f_1 et f_2 (telles celles représentées ci-dessous), telles qu'en tout point $x \in [0, 1]$, une des deux au moins s'annule, sont telles que $f_1 f_2 = 0$ avec $f_1 \neq 0$, $f_2 \neq 0$, 0 représentant évidemment l'élément neutre de la première opération, c'est-à-dire la fonction nulle sur tout l'intervalle.



Observons qu'*un corps est un anneau d'intégrité*.

En effet, si : $ab = 0$ avec $a \neq 0$, l'existence de l'inverse a^{-1} de a permet d'écrire :

$$a^{-1}ab = 0,$$

qui entraîne $b = 0$.

Exercice 38. — Réciproquement, tout anneau intègre fini est un corps.

Exercice 39. — Montrer que l'anneau des polynômes A[x] est un anneau d'intégrité si et seulement si l'anneau A est un anneau d'intégrité.

3. Anneaux de Boole.

Nous avons vu en exercice (n° 4) que les parties d'un ensemble formaient un anneau par rapport à la différence symétrique et à l'intersec-

tion. Cet anneau possède la particularité que la deuxième opération est telle que :

$$a \cap a = a.$$

Quand un anneau possède cette propriété, on le qualifie d'anneau de Boole.

Exercice 40. — On considère un anneau dans lequel

$$\forall a \in A \qquad a^2 = a$$

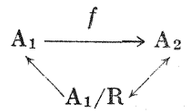
Démontrer que $a + a = 0$ et que l'anneau est commutatif (étudier le carré de $a + b$).

Si cet anneau possède au moins trois éléments il a des diviseurs de zéro.

Montrer qu'en fait il ne peut posséder trois éléments mais deux ou au moins quatre et qu'il existe une seule structure d'anneau de Boole à quatre éléments.

§ 3. HOMOMORPHISME SUR LES ANNEAUX. NOTION D'IDEAL

Nous reprenons notre schéma de tout à l'heure :



où, cette fois, les ensembles E et $F = f(E)$ ont la structure d'anneau et nous étudierons la relation R.

f, homomorphisme d'anneau, est déjà un homomorphisme pour les groupes additifs qui font partie de cette structure. Donc :

$$x \mathrm{R} y \iff x - y \in f^{-1}(0),$$

et $f^{-1}(0)$ est un sous-groupe additif de A. Mais, en outre, 0 représentant toujours l'élément neutre (1re opération) de A_2, on doit avoir :

$$\forall a_2 \in A_2 \quad 0a_2 = a_2 0 = 0.$$

Or, l'homomorphisme relatif à la deuxième opération entraîne donc que si $x \in f^{-1}(0)$, son produit à droite et à gauche par un élément quelconque a doit appartenir à $f^{-1}(0)$, puisque :

$$f(x)f(a) = 0f(a) = 0, \qquad f(a)f(x) = f(a)0 = 0.$$

Nous avons donc mis en évidence les deux propriétés suivantes du sous-ensemble $\mathcal{J} = f^{-1}(0)$ d'un anneau A :

1) *c'est un sous-groupe par rapport à l'addition ;*
2) $\forall a \in A, \quad \forall x \in \mathcal{J} \qquad ax \in \mathcal{J} \qquad xa \in \mathcal{J}$.

Ces deux propriétés définissent ce que l'on nomme un idéal bilatère d'un anneau. La deuxième propriété peut aussi s'écrire :

$$A\mathcal{J} \subset \mathcal{J} \qquad \mathcal{J}A \subset \mathcal{J}.$$

Réciproquement : Si on donne un idéal bilatère $\mathcal{J}$ d'un anneau A, la relation :

$$x \mathrm{R} y \iff x - y \in \mathcal{J}$$

définit une partition de l'anneau tel que l'espace quotient ait une structure d'anneau image homomorphe de A par l'application canonique.

Vérifions-le. Nous savons déjà que R est une relation d'équivalence puisque $\mathcal{J}$ est par rapport à l'addition un sous-groupe, nécessairement invariant puisque l'addition sur A est commutative (1er axiome de la structure d'anneau). Une classe (mod. $\mathcal{J}$) s'écrit :

$$\dot{x} = \{ y \,;\, x - y \in \mathcal{J} \} = x + \mathcal{J}.$$

Sur l'ensemble de ces classes, on peut définir une addition :

$$\dot{x} + \dot{y} = \overline{\dot{x} + y},$$

et une multiplication :

$$\dot{x} \times \dot{y} = \dot{\overline{xy}},$$

ces opérations ne prenant un sens que si le résultat est indépendant du représentant de la classe considéré. Ceci se vérifie aisément ; en effet, soient :

$$x' \in \dot{x}, \; y' \in \dot{y}, \text{ c'est-à-dire } x' - x \in \mathcal{J}, \; y' - y \in \mathcal{J}$$
$$(x' + y') - (x + y) = (x' - x) + (y' - y) \in \mathcal{J},$$

donc :

$$\overline{\dot{x'} + y'} = \overline{\dot{x} + y},$$
$$x'y' - xy = (x' - x)y' + x(y' - y) \in \mathcal{J},$$

donc :

$$\dot{\overline{x'y'}} = \dot{\overline{xy}}.$$

Il résulte de ces égalités que A/R est doté d'une structure d'anneau homomorphe de celle de A (les propriétés d'associativité, commutativité et distributivité « passant aux classes »).

Il sera appelé *anneau quotient modulo l'idéal* $\mathcal{J}$ *et noté* $A/\mathcal{J}$.

Remarque : Cet homomorphisme entraîne que si on fait la somme $\dot{x} + \dot{y}$ et le produit $\dot{x}\dot{y}$ en donnant à ces symboles le sens d'opérations sur l'ensemble des parties de l'ensemble A, tous les éléments des parties $\dot{x} + \dot{y}$ et $\dot{x}\dot{y}$ devront appartenir à la même classe ; donc, que $\dot{x} + \dot{y}$ et $\dot{x}\dot{y}$ devront être respectivement inclus dans $\overline{\dot{x} + y}$ et $\dot{\overline{xy}}$.

Réciproquement, ces inclusions prouvent que la somme (ou le produit) de tout $x \in \dot{x}$ et de tout $y \in \dot{y}$ appartient à une même classe, donc qu'on peut définir une opération sur les classes qui fait de l'espace quotient une image homomorphe de l'anneau. Ceci nous donne donc un autre moyen de démontrer l'homomorphisme précédent. Nous avons en effet pour $\dot{x} + \dot{y}$ et $\dot{x}\dot{y}$ au sens d'opérations sur les parties :

$$\dot{x} + \dot{y} = x + \mathcal{J} + y + \mathcal{J} = x + y + \mathcal{J} = \overline{x + y},$$

($\mathcal{J} + \mathcal{J} = \mathcal{J}$, puisque $\mathcal{J}$ est un sous-groupe),

et

$$\dot{x}\,\dot{y} = (x + \mathcal{J})(y + \mathcal{J}) = xy + x\mathcal{J} + \mathcal{J}y + \mathcal{J}^2,$$

or

$$x\mathcal{J} \subset \mathcal{J} \qquad \mathcal{J}y \subset \mathcal{J} \qquad \mathcal{J}^2 \subset \mathcal{J} \quad \text{donc} \quad \dot{x}\dot{y} \subset xy + \mathcal{J}$$
$$\dot{x}\dot{y} \subset \dot{\overline{xy}}$$

Il résulte donc de ceci que l'ambiguïté des notations (opération sur

les parties d'un ensemble ou opération sur les éléments de l'espace quotient) est sans importance pour la somme puisque le résultat est le même. Pour le produit où il y a seulement inclusion, il y aura lieu de préciser le point de vue adopté.

§ 4. PROPRIETES ELEMENTAIRES DES IDEAUX

1. Idéaux dans un corps. $\{0\}$ constitue un idéal puisque

$$\forall a \qquad 0a = 0 = a0.$$

Soit alors $a \neq 0$; un idéal contenant a contient son produit par a^{-1} ; il contient donc l'élément neutre de la 2e opération et, par conséquent, le produit de cet élément neutre par tout élément du corps, donc le corps tout entier. *Les seuls idéaux d'un corps sont* $\{0\}$ *et le corps tout entier.*

Dans le premier cas ($\mathcal{I} = \{0\}$), l'anneau quotient $K/\mathcal{I} = K$.

Dans le deuxième cas, l'anneau quotient est réduit à un seul élément.

Si l'on met à part ce 2e cas (c'est-à-dire celui des homomorphismes triviaux où tous les éléments de K sont envoyés sur un seul élément), on voit que les seuls corps qui puissent être images homomorphes de K sont ceux qui lui sont isomorphes. Il n'y a pas d'homomorphisme de corps qui ne soit un isomorphisme.

2. Exemples d'idéaux.

Idéaux de **Z**. Nous savons déjà que les seuls groupes additifs de **Z** sont de la forme $m\mathbf{Z}$. Eux seuls peuvent donc être des idéaux. On vérifie immédiatement qu'ils en sont en effet. L'ensemble quotient constitué par les entiers modulo m a donc une structure d'anneau commutatif.

> **Exercice 41.** — Montrer que cet anneau est un corps si et seulement si le nombre m est premier.

Idéaux dans les anneaux de polynômes.

Polynômes à coefficients dans un corps : $K[x]$.

Soit $\mathcal{I}$ un idéal de cet anneau et soit $B \in \mathcal{I}$ un des polynômes différents de 0, de $\mathcal{I}$, pris parmi ceux qui ont le plus petit degré.

Soit A un autre polynôme quelconque appartenant à $\mathcal{I}$. On sait qu'il existe deux polynômes Q et R à coefficients dans le même corps et tels que :

$$A = BQ + R \qquad d^\circ R < d^\circ B.$$

Or, $A \in \mathcal{I}$, $B \in \mathcal{I} \Rightarrow BQ \in \mathcal{I} \Rightarrow A - BQ \in \mathcal{I}$.

R de degré inférieur à celui de B devrait donc appartenir à $\mathcal{I}$, ce qui est contraire à l'hypothèse. Il faut donc que $R = 0$, donc que A soit un multiple de B. [Dans le cas où B serait une constante parmi les multiples de B il y aurait 1, produit de B par son inverse, et l'idéal se confondrait avec l'anneau tout entier]. Dans cet anneau comme dans **Z**, tous les idéaux sont formés par les multiples d'un élément de l'anneau.

Dans un anneau de polynômes à coefficients dans un anneau qui ne soit pas un corps, $\mathbf{Z}[x]$ par exemple, cette propriété, qui reposait sur l'existence d'une division avec reste, n'est plus vraie (voir exercice 42).

3. Construction des idéaux d'un anneau.

Observons d'abord que si on considère un anneau A et une famille d'idéaux de A, l'intersection de cette famille est encore un idéal. En particulier la famille des idéaux qui contiennent une partie B donnée n'est

pas vide (A lui appartient) ; l'intersection de cette famille est le plus petit idéal contenant B. On l'appelle idéal engendré par B.

En particulier, nous pourrons considérer les *idéaux engendrés par un élément.* Soit a un élément de l'anneau et (a) le plus petit idéal contenant a. Cherchons à le déterminer dans l'*hypothèse où l'anneau est commutatif.*

(a) doit d'abord contenir na, $\forall n \in \mathbf{Z}$.

Si l'anneau possède un élément unité e, ceci peut s'écrire :

$$ae + ae + \ldots\ldots + ae = a\underbrace{[e + e + \ldots\ldots + e]}_{n \text{ termes}} = a \times ne$$

ou si n est négatif $(-e - e \ldots - e)\, a = nea$,

et ne étant un élément de l'anneau, na est alors le produit de deux éléments de l'anneau. Mais si A n'est pas unitaire, na n'est pas le produit de deux de ses éléments. (a) doit aussi contenir xa pour tout x de A ; (a) doit donc contenir tous les éléments $na + xa$.

Or, on peut vérifier que l'ensemble de ces éléments forme un idéal car :

1) $na + xa + n'a + x'a = (n + n')\, a + (x + x')\, a$

et $-(na + xa) = (-n)\, a + (-x)\, a$

2) $(na + xa)\, x' = [a + \ldots\ldots + a]\, x' + xx'a$

$= ax' + \ldots\ldots + ax' + xx'a$

$= a\,[nx' + xx']$.

On peut donc conclure :

$$(a) = \{na + xa \,;\, n \in \mathbf{Z} \quad x \in A\}$$

et si A est unitaire, na étant un xa particulier,

$$(a) = \{xa \,;\, x \in A\}.$$

Un tel idéal est dit *principal* et un anneau, où tous les idéaux sont principaux, pourrait être dit un anneau principal. L'usage réserve, en fait, ce terme à ceux qui sont en outre intègres et unitaires. Les anneaux **Z** $K[x]$ sont donc des anneaux principaux.

Relation d'ordre sur l'ensemble des idéaux.

Observons que, dans un anneau principal,

$$(a) \subset (b) \iff b \mid a.$$

Par analogie, même dans un anneau non principal, on exprimera $\mathcal{I}_1 \subset \mathcal{I}_2$ en disant que $\mathcal{I}_2$ divise $\mathcal{I}_1$.

Les idéaux d'un anneau forment un treillis. En effet, leur ensemble peut être ordonné par inclusion et on aura :

$$\mathcal{I}_1 \cap \mathcal{I}_2 = \inf(\mathcal{I}_1, \mathcal{I}_2).$$

En conservant le langage que l'on vient d'indiquer, l'idéal ainsi défini sera qualifié de *P.P.C.M. des 2 idéaux.*

Pour ce qui est du sup, il faut observer que $\mathcal{I}_1 \cup \mathcal{I}_2$ n'est pas un idéal (la somme d'un élément de $\mathcal{I}_1$ et d'un élément de $\mathcal{I}_2$ n'appartient pas à $\mathcal{I}_1 \cup \mathcal{I}_2$), mais $\mathcal{I}_1 + \mathcal{I}_2$ en est un, et c'est le plus petit qui puisse contenir $\mathcal{I}_1$ et $\mathcal{I}_2$. C'est donc le sup de $\mathcal{I}_1$ et $\mathcal{I}_2$ et on l'appelle le *P.G.C.D. des 2 idéaux.*

Dans un anneau principal, l'idéal P.G.C.D. et l'idéal P.P.C.M. sont eux-mêmes des idéaux principaux et on a :

$$(a) \cap (b) = (m) \qquad (a) + (b) = (d),$$

les éléments m et d générateurs de (m) et (d) sont appelés respectivement P.P.C.M. et P.G.C.D. de a et de b et, dans les anneaux tels que **Z** ou $\mathbf{R}[x]$, ce P.P.C.M. et ce P.G.C.D. sont identiques à ceux définis élémentairement.

Ceci entraîne que d est un élément de $(a) + (b)$:

$$\exists \lambda, \mu \in A \qquad d = \lambda a + \mu b ;$$

appliqué à $\mathbf{Z}$ ou à $\mathbf{R}[x]$, ceci constitue le théorème de Bezout.

En particulier si a et b sont premiers entre eux :

$$(a) + (b) = (1) = A$$
$$\exists \lambda, \mu \in A \qquad \lambda a + \mu b = 1.$$

Mais si l'anneau n'est pas principal, il n'existe pas d'élément générateur unique du P.P.C.M. et du P.G.C.D.

Exercice 42. — Dans $\mathbf{Z}[x]$ l'idéal engendré par $x^2 + 1$ et $2x$ n'est pas un idéal principal.

Exercice 43. — Dans l'anneau $A = 2\mathbf{Z}$ des entiers pairs on considère l'idéal principal (4) ; montrer que l'inclusion

$$(4) A \subset (4)$$

est stricte.

Montrer que l'ensemble des multiples de (4) [multiple de 4 = produit de 4 par un élément de A] est un idéal I distinct de (4) et que pour cet idéal l'inclusion

$$AI \subset I$$

est stricte.

4. Idéaux premiers et Idéaux maximaux.

Soit un anneau A et $\mathcal{I}$ un idéal bilatère de A. Nous allons caractériser maintenant les idéaux qui donnent à l'anneau quotient $A/\mathcal{I}$ des structures remarquables. Cherchons d'abord *à quelles conditions $A/\mathcal{I}$ est un anneau d'intégrité.*

Dire que $A/\mathcal{I}$ est un anneau d'intégrité, c'est dire que :

$$\left.\begin{array}{l} \dot{a}\,\dot{b} = \dot{0} \\ \dot{a} \neq \dot{0} \end{array}\right\} \Rightarrow \dot{b} = \dot{0}.$$

Les lettres surmontées de points désignant comme précédemment les éléments de $A/\mathcal{I}$, c'est-à-dire les classes mod $\mathcal{I}$ ($\dot{a}$, classe contenant a..., etc...). Cette propriété est équivalente à la suivante :

$$\left.\begin{array}{l} ab \in \mathcal{I} \\ a \notin \mathcal{I} \end{array}\right\} \Rightarrow b \in \mathcal{I}.$$

Un idéal qui vérifie cette propriété est par définition *un idéal premier.*

Ce nom se justifie par ce qui se passe dans $\mathbf{Z}$. Tout idéal y est de la forme $(m) = \{ km \ ; k \in \mathbf{Z} \}$ et $a \in (m)$ veut dire $m|a$. L'anneau quotient correspondant est constitué par les entiers mod m. Dire que (m) est un idéal premier c'est dire, en traduisant la définition précédente, que :

$$\left.\begin{array}{l} m|ab \\ \text{non } (m|a) \end{array}\right\} \Rightarrow m|b.$$

Cette propriété est caractéristique des nombres premiers. Les idéaux premiers de $\mathbf{Z}$ sont donc les idéaux engendrés par des nombres premiers. Nous avions d'ailleurs déjà vu cette propriété en exercice (n° 41). Il convient d'y ajouter l'idéal (0) qui est premier, puisque l'anneau quotient est $\mathbf{Z}$ tout entier qui est un anneau d'intégrité.

Remarque : Cette dernière propriété est évidemment générale. L'idéal (0) est idéal premier d'un anneau si, et seulement si, cet anneau est d'intégrité.

Exercice 44. — On dit qu'un idéal I est primaire si

$$\left.\begin{array}{l} a \notin I \\ ab \in I \end{array}\right\} \Rightarrow \exists \rho \in \mathbf{N} \qquad b^\rho \in I$$

1) Montrer que si I est primaire, dans A/I tout diviseur de 0 est nilpotent c'est-à-dire qu'une de ses puissances est nulle.

2) I étant un idéal primaire montrer que l'ensemble des éléments a de l'anneau qui possèdent la propriété

$$\exists \rho \in \mathbf{N} \qquad a^\rho \in I$$

est un idéal premier J qui contient I.

Cherchons maintenant *à quelles conditions $A/\mathcal{I}$ est un corps* (indiquons que nous excluons le cas où $\mathcal{I}$ serait A tout entier et $A/\mathcal{I}$ réduit à un élément. Nous ne considérerons que les idéaux $\mathcal{I} \neq A$ que nous appellerons idéaux propres de A).

En employant toujours les mêmes notations, si $A/\mathcal{I}$ est un corps c'est que :

$$\forall \dot{a} \in A/\mathcal{I} \quad \dot{a} \neq \dot{0} \qquad \forall \dot{b} \in A/\mathcal{I} \quad \exists \dot{x} \in A/\mathcal{I} \quad \dot{a}\,\dot{x} = \dot{b}.$$

(Il existe aussi $\dot{y}$ tel que $\dot{y}\dot{a} = \dot{b}$, mais nous n'en aurons pas besoin).

Traduisons encore cette définition en revenant aux éléments de A. Il vient :

$$\forall a \in A \quad a \notin \mathcal{I}, \quad \forall b \in A \quad \exists x \in A \quad b - ax \in \mathcal{I},$$

ou encore, sous les mêmes hypothèses :

$$\exists x \in A \quad \exists r \in \mathcal{I} \quad b = ax + r.$$

Le fait que $A/\mathcal{I}$ est un corps entraîne donc que pour un a fixe n'appartenant pas à $\mathcal{I}$, tout $b \in A$ peut se mettre sous la forme $ax + r$, ce qui exige que r décrivant $\mathcal{I}$ et x décrivant A, $ax + r$ décrive tout A.

Mais si nous considérons le plus petit idéal qui contient $\mathcal{I}$ et a, tous les $ax + r$ lui appartiennent ; ce plus petit idéal contient l'ensemble des $ax + r$; il doit donc contenir A. La propriété de $\mathcal{I}$ qui est apparue est donc la suivante :

Un idéal contenant $\mathcal{I}$ et un élément $a \notin \mathcal{I}$ est A tout entier, et ceci quel que soit a ; autrement dit, il n'existe pas d'idéal contenant strictement $\mathcal{I}$ et qui ne soit A tout entier. Si nous considérons l'ensemble des idéaux propres de A ordonné par inclusion, nous voyons que $\mathcal{I}$ est un élément maximal (I. 2, 15) de cet ensemble. Un tel idéal est dit maximal et nous énoncerons :

Pour que $A/\mathcal{I}$ soit un corps, il est nécessaire que $\mathcal{I}$ soit un idéal maximal.

Cette condition n'est, à elle seule, pas suffisante.

Nous démontrerons seulement que :

Si A est anneau commutatif à élément unité et si $\mathcal{I}$ est un idéal maximal, $A/\mathcal{I}$ est un corps.

Ce que nous devons démontrer, c'est que $\dot{a}\dot{x} = \dot{b}$ admet une solution pour tout $\dot{a} \neq \mathcal{I}$ et tout $\dot{b}$, c'est-à-dire que :

$$\forall a \in A \quad a \notin \mathcal{I} \quad \forall b \in A \quad \exists x \in A \quad \exists r \in \mathcal{I} \quad b = ax + r.$$

L'hypothèse $\mathcal{I}$ maximal entraîne que l'idéal qui contient $\mathcal{I}$ et a soit A. Or, nous savons que si A est commutatif et unitaire, le plus petit idéal contenant a est $(a) = \{ xa \ ; x \in A \}$ et le plus petit idéal contenant $\mathcal{I}$ et a est :

$$\mathcal{I} + (a).$$

L'hypothèse $\mathcal{I}$ maximal s'écrit donc : $\mathcal{I} + (a) = A$ et signifie que $ax + r$ décrit tout A quand x décrit A et r décrit $\mathcal{I}$. La propriété est donc établie.

Un corps étant un anneau d'intégrité, *dans un anneau commutatif et unitaire un idéal maximal est premier.*

Réciproquement, nous allons montrer que, *dans un anneau principal commutatif, un idéal premier est maximal.* Soit (p) un idéal premier engendré par l'élément $p \neq 0$ et soit $a \in A$, $a \notin (p)$. Nous allons montrer que le plus petit idéal contenant (p) et a est l'anneau A tout entier, en montrant que l'élément unité 1 appartient à cet idéal. Puisque l'anneau est principal, cet idéal est engendré par un élément c et nous le notons (c) ; p lui appartenant, on a :

$$p = \lambda c, \text{ mais alors } \lambda c \in (p).$$

Or, c ne peut appartenir à (p) car $a \in (c)$, donc $a = kc$; si on avait $c = hp$ on aurait $a = khp$ donc $a \in (p)$, ce qui est contraire à l'hypothèse.

Donc, $\lambda c \in (p)$, $c \notin (p)$; la définition des idéaux premiers permet de conclure $\lambda \in (p)$ ou $\lambda = \mu p$, c'est-à-dire $p = \mu p c$,
ce qui, puisque l'anneau est unitaire, peut s'écrire :

$$p(1 - \mu c) = 0.$$

L'anneau étant d'intégrité et $p \neq 0$, il vient $\mu c = 1$, donc 1 appartient à (c).

Nous allons voir en exercice quelques contre-exemples prouvant la nécessité de certaines des hypothèses utilisées.

Exercice 45. — Dans $\mathbf{Z}[x]$, anneau des polynômes à coefficients entiers l'idéal engendré par $x^2 + 1$ est premier, non maximal (il s'agit ici d'un anneau qui n'est pas principal).

Exercice 46. — Dans $2\mathbf{Z}$: 1) Montrer que tout idéal est principal. 2). Déterminer les idéaux maximaux et montrer que pour l'un d'eux, $\mathcal{I}$, l'anneau quotient $2\mathbf{Z}/\mathcal{I}$ n'est pas un anneau d'intégrité (il s'agit ici d'un anneau qui n'est pas unitaire).

D'autre part, nous énoncerons sans démonstration (celle-ci exige l'axiome de Zermelo) le théorème de Krull : dans un anneau unitaire, tout idéal propre est contenu dans un idéal maximal. L'exercice qui suit nous fournira, au contraire, un exemple d'anneau (sans élément unité) où il n'y a pas d'idéal maximal.

Exercice 47. — On considère l'anneau $\mathcal{A}$ des polynômes fractionnaires à coefficients dans un anneau A commutatif. Un élément de cet anneau est une famille $\{a_r\}$ d'éléments de A indexés par $\mathbf{Q}+ - \{0\}$ (ensemble des rationnels strictement positifs) mais dont tous les éléments sont nuls sauf un nombre fini d'entre eux. L'addition est définie par

$$\{a_r\} + \{b_r\} = \{a_r + b_r\}$$

la multiplication par

$$\{a_r\}\{b_r\} = \left\{\sum_{s+t=r} a_s b_t\right\}$$

On peut utiliser aussi la notation suivante pour désigner un tel polynôme $\Sigma a_r x^r$; on a alors :

$$\Sigma a_r x^r + \Sigma b_r x^r = \Sigma (a_r + b_r) x^r$$

$$(\Sigma a_r x^r)(\Sigma b_r x^r) = \Sigma \left(\sum_{s+t=r} a_s b_t x^r \right)$$

les sommes étant étendues à tous les éléments r de $\mathbf{Q}+ - \{0\}$.

1) Vérifier que les lois indiquées font de un anneau commutatif sans élément unité.

2) Si on suppose que A a un élément unité, si x^r est le polynôme ($a_r = 1$, $a_s = 0$ pour $s \neq r$), montrer que si un idéal contient x^r, il contient x^s pour $s > r$.

3) Montrer que si un idéal $\mathcal{I}$ n'est pas $\mathcal{A}$ tout entier il existe des valeurs r tel que $x^r \notin \mathcal{I}$. En déduire qu'il existe dans $\mathcal{A}$ des idéaux qui ne sont contenus en aucun idéal maximal.

Exemple d'idéal maximal : Sur l'anneau des fonctions continues sur $[0, 1]$, l'ensemble $\mathcal{I}(x_0)$ des fonctions nulles pour la valeur x_0 constitue un idéal. Cet idéal est maximal ; en effet, si on considère l'idéal qui contient $\mathcal{I}(x_0)$ et une fonction f quelconque n'appartenant pas à $\mathcal{I}(x_0)$, cet idéal est l'anneau tout entier car toute fonction g peut se mettre sous la forme :

$$g = f\frac{g(x_0)}{f(x_0)} + \underbrace{g - f\frac{g(x_0)}{f(x_0)}}_{\varphi} = f\frac{g(x_0)}{f(x_0)} + \varphi$$

φ appartenant à $\mathcal{I}(x_0)$ puisque $\varphi(x_0) = 0$.

Exercice 48.. — Soient A_1 et A_2 deux anneaux et f un homomorphisme de A_1 dans A_2.

1) Montrer que l'image réciproque par f d'un idéal bilatère I_2 de A_2 est un idéal bilatère de A_1.

En particulier si A_1 est un sous-anneau de A_2 et I_2 un idéal bilatère de A_2, $A_1 \cap I_2$ est un idéal bilatère de A_1.

Que peut-on dire de

$$A_1/f^{-1}(I_2) \text{ et } A_2/I_2$$

1) si f est surjectif ?
2) si f ne l'est pas ?
3) montrer que si I_2 est premier, $f(I_2)$ l'est aussi.

§ 5. PLONGEMENT D'UN ANNEAU COMMUTATIF DANS UN CORPS

Un anneau A commutatif étant donné, peut-on trouver un corps K dans lequel A soit inclus et dont les deux opérations induisent sur A ses deux opérations ?

Une condition apparaît immédiatement comme nécessaire, c'est que A soit sans diviseurs de zéro puisqu'un corps est sans diviseur de zéro. Cette condition est suffisante. En effet, plonger un anneau dans un corps revient à plonger un ensemble muni d'une multiplication associative et commutative dans un groupe multiplicatif. Nous savons que c'est possible si A est un demi-groupe multiplicatif (II, 6, 1), ce qui exige que la multiplication soit simplifiable :

$$ax = ay \Rightarrow x = y,$$

or, il en est justement ainsi puisque A est un anneau d'intégrité
$(ax = ay \iff a(x - y) = 0 \Rightarrow x = y)$.

Le groupe multiplicatif est formé des classes d'équivalence des couples (a, b) d'éléments de A, la relation d'équivalence étant définie par :

$$(a, b) \sim (c, d) \iff ad = bc.$$

Il resterait à montrer qu'on peut définir entre les éléments de ce groupe une addition par rapport à laquelle la multiplication soit distributive et qui induise sur A l'addition de A.

C'est ce que nous avons fait (exercice 35) pour l'anneau $\mathbf{Z}$ des entiers et la construction du corps $\mathbf{Q}$ des rationnels. Le raisonnement serait le même pour un autre anneau. Nous en concluons que tout anneau d'intégrité commutatif peut être plongé dans un corps que nous appellerons le *corps des quotients de l'anneau d'intégrité.* Ce corps que nous avons déterminé est le plus petit corps contenant l'anneau A. Il est déterminé d'une manière unique à un isomorphisme près.

Exemple : Nous avons vu que $A[x]$ était un anneau d'intégrité si A était un anneau d'intégrité (exercice 39). L'anneau des polynômes $A[x, y]$

à deux variables et à coefficients dans A peut être considéré comme un anneau de polynômes à une variable y et à coefficient dans $A[x]$; $A[x]$ étant un anneau d'intégrité, $A[x, y]$ le sera aussi. Nous verrons ainsi, de proche en proche, que quand A est anneau d'intégrité, $A[x_1, x_2 \ldots x_n]$, anneau des polynômes à n variables, est encore un anneau d'intégrité. Pour tous ces anneaux, on pourra définir le corps des quotients appelés corps des fractions rationnelles. (Ils admettent tous comme sous-corps le corps des quotients de A).

Exercice 49. — On a vu que dans un corps K il n'y a d'idéaux que $\{0\}$ et K. On veut étudier la réciproque : on va montrer que si dans un anneau A, $\{0\}$ et A sont les seuls idéaux à gauche (un idéal à gauche est un sous-groupe additif de A qui vérifie $AI \subset I$) il n'y a que deux possibilités :

α) A est un anneau de carré nul c'est-à-dire $A^2 = \{0\}$ ($\forall a\ \forall b \in A$, $ab = 0$) et A n'a pas de sous-groupe non trivial.

β) A est un corps.

On montrera :

1) que dans un anneau, pour tout élément a de A, Aa est un idéal à gauche ;

2) supposant que α) n'est pas réalisée on prouvera qu'il existe un élément a tel que $Aa \neq \{0\}$ et un élément e tel que $ea = a$.

On étudiera alors les ensembles

$$\{x - xe\ ;\ x \in A\}$$
$$\{x - ex\ ;\ x \in A\}$$

et on conclura.

§ 6. CORPS

1. Corps premier.

L'intersection de tous les sous-corps d'un corps K est un sous-corps de ce corps K. Dans tout corps K il existe donc un sous-corps qui n'a pas de sous-corps propre, c'est-à-dire distinct de lui-même et de $\{0\}$. On le nomme corps premier.

Construction d'un corps premier. Notion de caractéristique.

Un corps premier k contient déjà au minimum 0 et e ; il contient $n\,e$ ($n \in \mathbf{Z}$) ; il contient les sommes d'éléments de cette nature :

$$ne + me = (n + m)\,e.$$

Il contient les produits d'éléments de cette nature, soit :

pour $m > 0$ $n > 0$ $\quad me \times ne = \underbrace{(e + \ldots + e)}_{m \text{ termes}}\ \underbrace{(e + \ldots + e)}_{n \text{ termes}} = mne^2 = mne$

pour $n > 0$ $m < 0$ $\quad me \times ne = \underbrace{(-e \ldots . - e)}_{m \text{ termes}}\ \underbrace{(e + \ldots . + e)}_{n \text{ termes}}$
$$= (-m)n(-e^2) = (-m)n(-e) = mne$$

pour $m < 0$ $n < 0$ $\quad me \times ne = \underbrace{(-e \ldots . - e)}_{m \text{ termes}}\ \underbrace{(-e \ldots . - e)}_{n \text{ termes}} =$
$$= (-m)\,(-n)e^2 = mne.$$

Nous considérons alors l'application φ de $\mathbf{Z}$ dans k, définie par :

$$n \xrightarrow{\varphi} ne$$

Cette application est un homomorphisme d'anneau puisque :

$$\varphi(m + n) = \varphi(m) + \varphi(n)$$
$$\varphi(mn) \quad = \varphi(m) \quad \varphi(n).$$

$\varphi(\mathbf{Z})$, image homomorphe de $\mathbf{Z}$, est donc un anneau isomorphe à un anneau quotient de $\mathbf{Z}$ modulo un idéal $\mathfrak{p}$. D'autre part, $\varphi(\mathbf{Z})$, devant être un sous-anneau d'un corps, ne peut avoir de diviseurs de 0. Il faut donc que $\mathfrak{p}$ soit un idéal premier de $\mathbf{Z}$. Or, on sait que les seuls idéaux premiers de $\mathbf{Z}$ sont les idéaux engendrés par un nombre premier et l'idéal (0). Il n'y a donc pour $\varphi(\mathbf{Z})$ que deux types de structure possibles :

1) $\mathfrak{p}$ est engendré par un nombre premier p ; l'anneau quotient est l'anneau des entiers modulo p qui est un corps ; $\varphi(\mathbf{Z})$ étant isomorphe à un corps est le corps premier k cherché.

2) $\mathfrak{p}$ est l'idéal (0) ; $\mathbf{Z}/\mathfrak{p} = \mathbf{Z}$; $\varphi(\mathbf{Z})$ est isomorphe à l'anneau des entiers. Le plus petit corps qui le contienne est donc isomorphe à $\mathbf{Q}$.

Tout corps premier est donc isomorphe à l'un des corps suivants :

1) *corps des rationnels ;*
2) *corps des entiers modulo p (premier).*

Il y a lieu de remarquer qu'ils sont tous commutatifs. Dans le premier cas, on dit que le corps est de *caractéristique nulle ;* dans le deuxième, qu'il est de *caractéristique p.* Et on appelle caractéristique d'un corps quelconque la caractéristique de son corps premier.

Dans un corps de caractéristique p, $\forall a \quad pa = 0$

En effet, le corps contenant un sous-corps isomorphe aux entiers modulo p, on a :

$$pe = 0$$

et

$$pa = \underbrace{a + a + \ldots . . a}_{p \text{ termes}} = \underbrace{ae + ae + \ldots . . + ae}_{p \text{ termes}}$$
$$= a\underbrace{[e + \ldots . . . . + e]}_{p \text{ termes}} = a \times pe = 0.$$

Il résulte de là que les règles du calcul algébrique dans un corps de caractéristique p sont très différentes de celles du calcul algébrique habituel (corps des réels ou corps des complexes, admettant Q comme corps premier et ayant pour caractéristique 0). Soit par exemple à développer $(x + y)^p$. Le développement formel du binôme reste valable, mais tous les C_p^k pour $k \neq 0$, $k \neq p$ et pour p premier sont des entiers divisibles par p. (Dans la fraction $C = \dfrac{p\,(p-1)\ \ldots\ (p-k+1)}{k\,!}$, aucun des facteurs du dénominateur, inférieurs à p, ne peut diviser le nombre premier p). Donc, dans un corps de caractéristique $p \neq 0$, on a :

$$(x + y)^p = x^p + y^p.$$

2. Extension des corps.

Dans tout ce qui va suivre, nous supposerons toujours que nous sommes en présence de corps *commutatifs.* Nous commencerons par nous placer dans la situation suivante : soit un corps K et un corps E dont K est un sous-corps :

$$K \subset E$$

(on dit aussi que E est un sur-corps de K).

Soit alors A une partie de E. Tous les corps contenus dans E et contenant K et A ont pour intersection un sous-corps de E qui est le plus petit sous-corps contenant K et A ; nous l'appellerons le *corps engendré par* A et le noterons K(A).

$$E \supset K(A) \supset K \qquad E \supset K(A) \supset A.$$

Cherchons à construire K(A).

K(A) doit contenir les éléments de A, les puissances de ces éléments, puis les polynômes P à coefficients dans K et à valeurs dans A, et enfin les fractions rationnelles $\frac{P}{Q}$ avec $Q \neq 0$ (*). K(A) doit donc contenir l'ensemble de ces fractions rationnelles. Or, cet ensemble forme un corps, comme on le vérifie immédiatement (**). Ce corps contient A et contient K, donc c'est K(A).

Portons maintenant notre attention sur l'ensemble de ces fractions rationnelles qui ne contiennent qu'un ensemble fini $B = \{ u_1 \dots u_p \}$ d'éléments de A. Leur ensemble forme le corps le plus petit contenant B et K et est donc K(B). Si nous considérons alors tous les B possibles, c'est-à-dire si B décrit l'ensemble

$$\mathcal{P}_f(A)$$

des parties finies de A, nous obtenons un ensemble de sous-corps K(B). Tous sont inclus dans K(A), leur réunion l'est donc aussi ; mais, réciproquement, toute fraction rationnelle appartenant à K(A) contient un nombre fini d'éléments de A, donc appartient à celui des K(B) qui correspond à cet ensemble d'éléments. On peut donc écrire :

$$K(A) = \bigcup \{ K(B) \ ; \ B \in \mathcal{P}_f(A) \} .$$

Il en résulte que, pour trouver K(A), on peut commencer par chercher les corps engendrés par une partie finie de A.

Exercice 50. — Soit un corps E et une famille $\mathcal{K}$ de sous-corps de E telle que

$$\forall K_1, K_2 \in \mathcal{K} \qquad \exists K \in \mathcal{K} \qquad K_1 \subset K \qquad K_2 \subset K$$

pour une telle famille

$$\bigcup \qquad \in \mathcal{K} \}$$

est un corps.

Dans la construction du corps engendré par une partie finie de A, nous allons être aidés par la propriété suivante : soient $A_1 \subset E$, $A_2 \subset E$ et leur union $A_1 \cup A_2$. $K(A_1)$ est un sous-corps de E ; son extension engendrée par la partie A_2, que nous noterons $K(A_1)(A_2)$, est identique au corps $K(A_1 \cup A_2)$.

En effet, $K(A_1)(A_2)$ contient K, A_1, A_2, donc $A_1 \cup A_2$, donc :

$$K(A_1)(A_2) \supset K(A_1 \cup A_2).$$

Mais, d'autre part, $K(A_1 \cup A_2)$ contient A_2 et contient $K(A_1)$, puisque A_1 est une partie de $A_1 \cup A_2$; $K(A_1 \cup A_2)$ contenant A_2 et $K(A_1)$ contient $K(A_1)(A_2)$ qui est le plus petit corps qui les contienne.

$$K(A_1 \cup A_2) \supset K(A_1)(A_2).$$

Les deux inclusions opposées donnent l'égalité :

$$K(A_1)(A_2) = K(A_1 \cup A_2)$$

(*) Il importe de bien préciser qu'il ne s'agit pas de polynômes ou de fractions rationnelles formels, mais d'éléments de E, qui sont les valeurs prises par ces polynômes ou fractions rationnelles. En particulier, $Q = 0$ ne signifierait pas qu'il s'agit de l'élément nul de l'anneau des polynômes, mais de l'élément nul de E, valeur prise par le polynôme Q.

(**) C'est ici qu'intervient l'hypothèse de commutativité ; car les monômes $a_i u_i^k$ et $a_j u_j^h$ n'ont pour produit le monôme $a_i a_j u_i^k u_j^h$ que dans cette hypothèse.

Ceci nous permet de construire en deux temps $K(A_1 \cup A_2)$ par adjonctions successives de A_1 et de A_2. Cela prouve en même temps que l'ordre dans lequel se font ces adjonctions n'influe pas sur le résultat.

Pour former le corps engendré par la partie finie $B = \{ u_1, \dots, u_p \}$, on pourra donc former $K(u_1)$, puis $K(u_1)(u_2)$..., etc... Tout revient donc à construire $K(\theta)$, corps engendré par un seul élément. Une telle extension est dite simple.

3. Extensions simples.

Soient donc un corps E et K un sous-corps de E, θ un élément de E n'appartenant pas à K ($\theta \in K \Rightarrow K(\theta) = K$), $K(\theta)$ contient tous les polynômes en θ à coefficients dans K dont nous désignons l'ensemble par $K[\theta]$. Les règles de calcul sur ces polynômes sont les mêmes que celles sur les polynômes de l'anneau $K[x]$ des polynômes à une indéterminée et à coefficients dans K. On peut donc considérer l'application :

$$K[x] \xrightarrow{f} K[\theta] \subset K(\theta),$$

qui est un homomorphisme d'anneaux. $K[\theta]$, image homomorphe d'un anneau, est isomorphe à l'anneau quotient de $K[x]$ par l'idéal :

$$\mathcal{I} = f^{-1}(0).$$

Cet idéal est constitué par l'ensemble des polynômes P de $K[x]$ tels que :

$$P(\theta) = 0.$$

Nous devons donc chercher à préciser cet idéal ; mais $K[\theta]$ étant inclus dans un corps est un anneau sans diviseur de zéro ; donc, $K[x]/\mathcal{I}$ l'est aussi ; c'est-à-dire que $\mathcal{I}$ est un idéal premier de $K[x]$.

$K[x]$ étant un anneau d'intégrité (ceci a été démontré dans l'exercice 39), l'idéal $\{ 0 \}$ y est un idéal premier, $(K[x]/\{ 0 \} = K[x])$. Nous pouvons donc avoir $\mathcal{I} = 0$ ou bien $\mathcal{I}$ idéal premier différent de $\{ 0 \}$. Considérons séparément ces deux cas :

1) $\mathcal{I} = \{ 0 \}$. L'homomorphisme f est un isomorphisme et $K[\theta]$ est un anneau d'intégrité qui n'est pas un corps. Le plus petit corps qui le contient est, comme nous l'avons montré (III, 5), le corps des quotients, c'est-à-dire $K(\theta)$, *corps des fractions rationnelles en θ à coefficients dans* K. Une telle extension est dite une *extension transcendante simple*. Ce cas est caractérisé par le fait que θ n'annule aucun polynôme de $K[x]$.

2) $\mathcal{I} \neq \{ 0 \}$. $K[x]$ étant un anneau principal (III, 4, 2), tout idéal premier y est maximal (III, 4, 4), et $K[x]/\mathcal{I}$ sera un corps. $K[\theta]$ qui lui est isomorphe est un corps ; et, dans ce cas, le corps $K(\theta)$ n'est autre que $K[\theta]$. Une telle extension est une *extension algébrique simple*. $\mathcal{I}$ est un idéal principal ; tous les polynômes qui lui appartiennent sont donc les multiples d'un polynôme p tel que :

$$p(\theta) = 0.$$

Ce polynôme p est irréductible, ce qui veut dire qu'il ne peut exister deux polynômes p_1 et p_2 (à coefficients dans K) non réduits à des constantes, tels que $p = p_1 p_2$, car, s'il existait deux tels polynômes, l'idéal engendré, par exemple par p_1, inclurait l'idéal $\mathcal{I}$ qui ne serait pas maximal.

Or, nous excluons le cas sans intérêt où p serait un polynôme du premier degré, car alors sa racine θ aurait déjà appartenu à K et $K(\theta)$ ne serait autre que K lui-même. Si donc, p est un polynôme de degré au moins égal à 2, que p soit irréductible, entraîne qu'aucun nombre

$x \in K$ n'annule p, donc que l'équation $p(x) = 0$ était sans solution dans le corps K (*).

Une extension algébrique simple se fait donc en ajoutant au corps K *un élément* θ *du corps* $E \supset K$ *qui est racine d'un polynôme* p *à coefficients dans* K, *irréductible* (*et par conséquent sans racines*) *dans* K. Cette extension $K(\theta)$ est isomorphe à l'anneau quotient de $K[x]$ par l'idéal engendré par ce polynôme p.

$$K(\theta) \approx K[x]/(p).$$

Examinons la structure de cet anneau quotient (qui est un corps). Si n est le degré de p, il existe dans chaque classe (mod. p) de $K[x]$ un polynôme de degré inférieur à n, car tout polynôme est congru (mod. p) au reste de sa division par p ; et, dans chacune de ces classes, il existe un seul polynôme de degré inférieur à n, la différence de deux tels polynômes ne pouvant être divisible par p. Chaque classe peut donc être représentée par un polynôme de degré inférieur à n et $K(\theta)$ peut être représenté par l'ensemble des polynômes en θ à coefficients dans K et de degré inférieur à n. La somme de deux éléments $g(\theta)$ et $h(\theta)$ s'obtient en faisant la somme des polynômes formels g et h et, en prenant $(g + h)(\theta)$; pour le produit $g(\theta) \times h(\theta)$, on fera le produit gh, puis, si son degré atteint ou dépasse n, on prendra le reste de la division par p, c'est-à-dire que si :

$$gh = pq + r \qquad r^0 < n,$$

on aura :

$$g(\theta) \times h(\theta) = r(\theta).$$

Ceci revient à dire qu'on calcule sur les éléments de $K(\theta)$ comme sur les polynômes formels de $K[x]$, mais en remplaçant $p(\theta)$ par 0.

Remarque : Le fait que $K(\theta)$ soit un corps prouve pour tout $g(\theta)$ l'existence de $h(\theta)$ tel que :

$$\frac{1}{g(\theta)} = h(\theta).$$

Quant au moyen de trouver cet élément $h(\theta)$, il peut nous être fourni par le théorème de Bezout (voir III, 4, 3), qui s'applique dans $K[x]$: p étant irréductible et g de degré inférieur à n, donc premier avec p, il existe k et h (polynômes à coefficients dans K) tels que :

$$kp + gh = 1,$$

ce qui se traduit (en vertu des règles de calcul ci-dessus énoncées) par :

$$g(\theta)h(\theta) = 1.$$

On appelle *degré de l'extension algébrique* le degré du polynôme p. $K(\theta)$ est isomorphe au groupe additif des polynômes en x de degré inférieur à n ; ces polynômes forment un espace vectoriel sur K et peuvent s'exprimer sous forme d'expressions linéaires des n éléments $1, \theta, \ldots, \theta^{n-1}$.

En anticipant un peu sur la théorie des espaces vectoriels, nous dirons que cet espace vectoriel est de dimension n puisqu'il admet la base $(1, \theta, \ldots, \theta^{n-1})$.

Autre point de vue. Nous avons jusqu'à maintenant cherché à étendre un corps K en lui adjoignant un élément qui appartenait au surcorps E de K déjà connu. Nous pouvons au contraire nous poser le problème suivant : étant donné seulement le corps K, peut-on fabriquer un corps $\widehat{K} \supset K$?

(*) Bien entendu, la notion d'irréductibilité d'un polynôme est relative à l'ensemble dans lequel on cherche à le factoriser. $x^4 + 1$, irréductible dans **Q**, est factorisable dans **R** puisqu'il peut s'écrire $(x^2 + x\sqrt{2} + 1)\ (x^2 - x\sqrt{2} + 1)$.

Il existe toujours une solution à ce problème : l'extension transcendante formée des fractions rationnelles à coefficients dans K ; elle est unique, ce qui veut dire que deux extensions transcendantes simples du même corps K sont isomorphes. Parmi les éléments de cette extension figure le polynôme formel $(0, 1, 0, \ldots, 0)$.

Si nous désignons cet élément par θ, tous les autres éléments de l'extension apparaîtront comme des fractions rationnelles en θ. Mais peut-on trouver des extensions algébriques ?

Oui, si on connaît des polynômes irréductibles dans $K[x]$, et on pourra construire autant d'extensions algébriques simples que $K[x]$ possède de polynômes p irréductibles [ces extensions peuvent être distinctes ou non]. Le polynôme $[0, 1, 0, \ldots, 0]$ (mod. p) étant encore désigné par θ, tous les éléments de l'extension peuvent être considérés comme des polynômes en θ (mod. p). *Le nouvel élément est racine du polynôme* p *qui, dans le nouveau corps, n'est plus irréductible.*

4. Exemples.

Construction des irrationnels algébriques. K est le corps des rationnels, **Q**. Prenons, par exemple, pour p :

$$p = x^2 - 2,$$

irréductible dans **Q**. L'extension $Q(\theta)$ est constituée par toutes les expressions $a\theta + b$, où a et b sont des rationnels et θ un nombre tel que :

$$\theta^2 - 2 = 0.$$

$(a\theta + b)\ (c\theta + d)$ est le reste de la division par $x^2 - 2$ de : $(ax + b)\ (cx + d)$, où on fait $x = \theta$, ce qui n'est autre que l'expression obtenue en remplaçant θ^2 par 2 dans l'expression précédente. De même :

$$\frac{a\theta + b}{c\theta + d} = \frac{(a\theta + b)(c\theta - d)}{(c\theta + d)(c\theta - d)} = \frac{2ac - bd}{2c^2 - d^2} + \theta\frac{bc - ad}{2c^2 - d^2}.$$

En définitive, on calcule avec le nombre θ comme avec les rationnels en remplaçant, chaque fois que l'occasion s'en présente, θ^2 par 2. Ce nombre θ est celui habituellement désigné par $\sqrt{2}$ (mais peut-être tout aussi bien $-\sqrt{2}$). Dans l'extension ainsi créée et notée conformément aux notations indiquées $Q(\sqrt{2})$, le polynôme $x^2 - 2$ se factorise en :

$$(x - \sqrt{2})\ (x + \sqrt{2}).$$

Il est clair qu'un certain nombre d'autres polynômes, irréductibles dans **Q**, « éclatent » (c'est-à-dire se factorisent en facteurs du premier degré) dans $Q(\sqrt{2})$.

Toutes les extensions quadratiques (c'est-à-dire toutes les extensions par rapport à des polynômes irréductibles du 2e degré) se feront de façon analogue et permettront de définir les racines carrées de tous les entiers.

Constructions des complexes. Prenons pour K le corps **R** des réels et pour p :

$$p = x^2 + 1.$$

Appelons i un des nombres θ correspondants :

$$i^2 + 1 = 0.$$

Nous calculerons sur les expressions du premier degré $ai + b$ de façon analogue à ce que nous avons fait ci-dessus, mais en remplaçant cette fois i^2 par -1.

Le polynôme $x^2 + 1$ se factorise en $(x + i)(x - i)$; mais, ce que nous apprend le théorème de d'Alembert, c'est que le corps des complexes, extension algébrique des réels ainsi construite, est un corps où tous les polynômes à coefficients réels se factorisent en polynômes du premier degré. Qui plus est, tous les polynômes à coefficients dans le nouveau corps y éclatent aussi. *On ne pourra donc construire aucune extension algébrique du corps des complexes.*

On dira de ce corps qu'il est *algébriquement clos.*

Les quatre propriétés suivantes, équivalentes entre elles, sont caractéristiques des corps algébriquement clos :

1) Aucun polynôme de degré supérieur à 1, à coefficients dans ce corps, n'est irréductible.

2) Tout polynôme non constant à coefficients dans ce corps est produit de polynômes du premier degré.

3) Tout polynôme à coefficient dans ce corps a au moins une racine dans ce corps.

4) Toute extension algébrique de ce corps est identique à lui-même.

Nombres algébriques ou trancendants. Un élément est dit transcendant par rapport à un corps K quand il n'est racine d'aucune équation à coefficients dans K ; on a pu démontrer que e et π sont transcendants par rapport à **Q**. L'extension simple correspondante est transcendante. (Le plus petit corps contenant **Q** et e est celui des fractions rationnelles en e).

Si, au contraire, un élément est racine d'un polynôme irréductible de degré n sans l'être d'aucun polynôme de degré inférieur à n, il est dit *algébrique de degré n* ; l'extension simple correspondante est une extension algébrique de degré n.

5. Factorisation d'un polynôme. Corps de décomposition.

Nous avons vu tout à l'heure deux exemples du cas où, ajoutant un élément au corps de ses coefficients, on rend possible l'éclatement d'un polynôme, c'est-à-dire du cas où, en ajoutant une racine, on les ajoute toutes. Il en sera ainsi pour toutes les extensions du second degré. En effet, le polynôme p du 2e degré se factorise en :

$$p = (x - \theta)(\alpha x + \beta) \qquad \alpha, \beta \in K(\theta).$$

Mais il peut ne pas en être ainsi. Par exemple, si on ajoute à **Q** une racine de $x^3 - 2$, les autres ne viennent pas en même temps. Cela amène à faire des extensions successives d'un même corps jusqu'au moment où nous arriverons à un corps dans lequel le polynôme donné se factorise en polynômes du premier degré. Le corps ainsi obtenu, qui est le *corps de factorisation totale du polynôme,* est appelé, en anglais, splitting field, et en français, suivant les auteurs, *corps des racines, corps de rupture* ou *corps de décomposition* du polynôme.

Or, un polynôme p étant factorisé en polynômes $p_1, p_2, \ldots$ de degrés supérieurs à 1, on peut faire d'abord une extension du corps de ses coefficients par rapport au polynôme p_1 ; on obtient une nouvelle factorisation ; si un des facteurs est encore de degré supérieur à 1, on fait une nouvelle extension, etc... ; mais on aurait pu commencer par faire une extension par rapport à p_2 et la question se pose alors de savoir si le résultat aurait été le même. La réponse est :

Le corps de factorisation totale d'un polynôme est déterminé à un isomorphisme près.

Pour établir cette propriété, nous montrerons d'abord comment un

isomorphisme de corps peut s'étendre aux extensions de ces corps. Soit un isomorphisme :

$$K \xrightarrow{\varphi} \overline{K}$$

Un polynôme p irréductible dans K est transformé par φ en un polynôme $\overline{p}$ irréductible dans $\overline{K}$ (chaque coefficient de $\overline{p}$ étant l'image du coefficient correspondant de p).

Les deux extensions sont respectivement isomorphes à :

$$K[x]/_{(p)} \qquad \text{et} \qquad \overline{K}[x]/_{(\overline{p})}$$

qui sont évidemment isomorphes.

Supposons alors qu'un polynôme à coefficients dans K éclate dans deux corps $\mathcal{K}$ et $\overline{\mathcal{K}}$, tous deux surcorps de K, en ayant dans le premier les racines $\alpha_1, \ldots, \alpha_n$ et dans le deuxième $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$ (leur nombre est le même, car c'est le degré de p). Nous nous trouvons dans la situation où nous étions au début de ce chapitre (1er point de vue) et nous allons construire les corps :

$$K(\alpha_1, \ldots, \alpha_n) \subset \mathcal{K} \quad \text{et} \quad K(\overline{\alpha_1}, \ldots, \overline{\alpha_n}) \subset \overline{\mathcal{K}}$$

Ces corps sont parfaitement déterminés et l'ordre dans lequel on ajoute les éléments n'intervient pas puisque $K(\alpha_1)(\alpha_2)$ et $K(\alpha_2)(\alpha_1)$ égalent $K(\alpha_1 \cup \alpha_2)$. Nous ajoutons donc d'abord α_1 et $\overline{\alpha_1}$ et obtenons deux extensions isomorphes $K(\alpha_1)$ et $K(\overline{\alpha_1})$.

Dans ces extensions, le polynôme p se factorise de façons isomorphes. Nous entendons par là que si :

$$p = (x - \alpha_1)(x - \beta_1) \ldots (x - \lambda_1)\, g h \ldots k,$$
$$p = (x - \overline{\alpha_1})(x - \overline{\beta_1}) \ldots (x - \overline{\lambda_1})\, \overline{g}\,\overline{h} \ldots \overline{k},$$

$\beta_1 \ldots \lambda_1$ et $\overline{\beta_1} \ldots \overline{\lambda_1}$ ont des expressions identiques respectivement par rapport à α_1 et $\overline{\alpha_1}$ et que les polynômes irréductibles $g, h, \ldots, k$ et $\overline{g}, \overline{h}, \ldots, \overline{k}$ sont identiques au remplacement près de α_1 par $\overline{\alpha_1}$ dans l'expression de leurs coefficients.

Les racines $\beta_1 \ldots \lambda_1$ sont parmi les nombres $\alpha_1 \ldots \alpha_n$, de même que $\overline{\beta_1} \ldots \overline{\lambda_1}$ sont parmi les nombres $\overline{\alpha_1} \ldots \overline{\alpha_n}$. En cherchant à construire $K(\alpha_1)$ et $K(\overline{\alpha_1})$, nous avons, en fait, construit les corps isomorphes :

$$K(\alpha_1 \ldots \alpha_k) \quad \text{et} \quad K(\overline{\alpha_1} \ldots \overline{\alpha_k}).$$

Puisque l'ordre dans lequel on fait les adjonctions n'intervient pas, nous choisissons d'ajouter maintenant les racines α_{k+1} et $\overline{\alpha_{k+1}}$ de p qui sont respectivement racines des polynômes isomorphes g et $\overline{g}$. Le lemme démontré ci-dessus s'applique alors et :

$$K(\alpha_1 \ldots \alpha_k \alpha_{k+1}) \approx K(\overline{\alpha_1} \ldots \overline{\alpha_k}\,\overline{\alpha_{k+1}}).$$

Nous considérerons alors les décompositions de p dans ces deux nouveaux corps et construirons de nouvelles extensions en introduisant deux racines de facteurs homologues... Et ainsi de suite jusqu'au moment où, en procédant par extensions successives et en ayant toujours deux corps isomorphes, nous obtiendrons deux corps de décomposition isomorphes.

Racines multiples. Une question qui se pose encore est la suivante : un polynôme irréductible dans K peut-il avoir dans sa décomposition dans l'extension $K(\theta)$ plusieurs facteurs du premier degré identiques ?

Soit :

$$p = (x - \theta)^{\lambda} q \qquad \text{avec } \lambda > 1.$$

Nous y répondrons dans l'exercice suivant :

Exercice 51. — La condition nécessaire et suffisante pour que θ soit une racine multiple d'un polynôme est que le corps K soit de caractéristique $c \neq 0$ et que

$$p \in K[x^c]$$

Pour les corps de caractéristique nulle (rationnels, réels, par exemple) θ sera toujours racine simple.

Exercice 52. — Dans le corps $\mathbf{Z}_2$ (entiers mod. 2) chercher tous les polynômes irréductibles de degré 2, 3, 4. Etudier la structure des extensions correspondantes.

Exercice 53. — Soient un corps et une indéterminée z, les corps $K(z)$ et $K\left(\frac{z^3}{z+1}\right)$ des fractions rationnelles en z et $\frac{z^3}{z+1}$. Le deuxième de ces corps est un sous-corps du premier. Montrer que le premier est une extension algébrique du second et trouver le polynôme irréductible par rapport auquel est faite cette extension.

Exercice 54. — Un surcorps E est dit algébrique sur K si tous les éléments de E sont algébriques sur K. La condition nécessaire et suffisante pour que E soit algébrique sur K est que si A est un anneau tel que $K \subset A \subset E$ (les opérations sur A étant induites par celles de E), alors A soit un corps.

Exercice 55. — Soit E un surcorps de K et A une partie de E algébrique sur K, c'est-à-dire dont tous les éléments sont algébriques par rapport à K. Montrer que K(A) est algébrique sur K.

Exercice 56. — Soient trois corps $K \subset E \subset F$. La condition nécessaire et suffisante pour que F soit algébrique sur K est que E soit algébrique sur K et F algébrique sur E. Dans ces conditions θ étant un élément de F comparer les deux polynômes p_E irréductible dans E et p_K irréductible dans K tels que

$$p_E(\theta) = 0 \qquad p_K(\theta) = 0$$

Exercice 57. — Tout corps fini a une caractéristique différente de 0 soit c. Montrer que :

1) un corps fini, de caractéristique c, a $q = c^n$ éléments avec n entier :
2) c'est le corps de décomposition du polynôme $x^q - x = 0$;
3) son groupe multiplicatif est cyclique.

CHAPITRE IV

NOMBRES RÉELS

§ 1. INVENTAIRE DES PROPRIETES DE Q

Les chapitres précédents ont mis en évidence les principales propriétés de **Q** :

1) C'est un corps commutatif.

2) Il jouit d'une *structure d'ordre total* compatible avec la structure de corps (*) et cet ordre est *archimédien* (II, 4, 3).

3) **Q** *est un espace métrique.*

Nous appelons *distance* sur **Q** l'application :

$$d : \mathbf{Q}^2 \longrightarrow \mathbf{Q}^+$$

définie par : $d(x, y) = |x - y|$.

Elle jouit des propriétés suivantes :

$$d(x, y) = 0 \iff x = y,$$

$$\forall x, \quad \forall y \qquad d(x,y) = d(y,x),$$

$$\forall x, \quad \forall y, \quad \forall z \qquad d(x, y) \leqslant d(x, z) + d(y, z) \text{ (inégalité triangulaire).}$$

Les deux premières de ces propriétés sont évidentes. La 3e a été démontrée (exercice 31).

Plus généralement, une distance sur un ensemble E sera une application d de E^2 dans $\mathbf{R}^+$ (ensemble que nous allons définir et qui contient $\mathbf{Q}^+$), d possédant les trois propriétés énumérées ci-dessus. Un ensemble muni d'une distance est dit un espace métrique (ou distancié).

Nous allons maintenant mettre en évidence certains aspects insuffisants de ces propriétés :

1) **Q** *n'est pas algébriquement clos.* $x^2 - 2$, $x^2 + 1$, par exemple, ne s'y factorisent pas. Dans ce chapitre, nous ne nous arrêterons pas à ce point de vue, car le corps des réels que nous allons construire n'est pas, lui non plus, algébriquement clos.

2) Comme tout ensemble muni d'un ordre total, **Q** est un treillis, mais ce *n'est pas un treillis complet.* Un ensemble E est dit un treillis complet si tout $A \in \mathcal{P}(E)$ possède un plus petit majorant qui est dit sup. A et un plus grand minorant qui est dit inf. A ; cette propriété entraîne que tout $A \in \mathcal{P}(E)$ possède des majorants et des minorants.

(*) Nous entendons par là que : 1) c'est un groupe additif ordonné (voir cours II. 4.1 et corrigé de l'exercice 35) ; 2) que le produit de deux éléments positifs est positif. Ceci, compte tenu de la structure de groupe additif ordonné et de la distributivité de la multiplication par rapport à l'addition, a entraîné la règle des signes.

Si, au contraire, on peut seulement affirmer l'existence de sup. A (resp. inf. A) pour ceux des $A \in \mathcal{P}(E)$ que l'on sait être majorés (resp. minorés), on dit alors que A est un treillis conditionnellement complet.

Observons qu'un groupe n'aura jamais une structure de treillis complet compatible avec sa structure de groupe. En effet, parmi les parties de E, il y a E lui-même ; donc, E aurait une borne supérieure qui serait un de ses éléments, a, et alors $a + x$ devrait être $\leqslant a$ pour tout $x \in E$, ce qui est impossible pour les éléments positifs x de E, et en particulier pour a si le groupe n'est pas réduit à 0.

Mais **Q** *n'est pas non plus un treillis conditionnellement complet.* Si nous considérons l'ensemble :

$$A = \{ r \in \mathbf{Q}^+ ; r^2 < 2 \},$$

ce sous-ensemble de **Q** possède pour majorants tous les éléments de :

$$A' = \{ s \in \mathbf{Q}^+ ; s^2 > 2 \},$$

mais cet ensemble A' ne possède pas de plus petit élément.

3) Dans un espace métrique, on est amené à se poser la question de la *convergence des suites.*

On nomme suite une famille d'éléments x_n indexés par les éléments de N et on dit qu'une suite converge vers une limite X si :

$$\forall \varepsilon \in \mathbf{R}^+ - \{0\} \quad \exists n_0 \in \mathbf{N} \quad \forall n > n_0 \quad d(X, x_n) < \varepsilon.$$

(Ici, la définition sera évidemment donnée avec $\forall \varepsilon \in \mathbf{Q}^+ - \{0\}$). On peut souhaiter donner de la convergence d'une suite un critère qui ne ferait pas intervenir la limite X. Or, l'inégalité triangulaire qui permet d'écrire :

$$d(x_n, x_m) < d(X, x_n) + d(X, x_m) < 2\varepsilon,$$

permet d'affirmer :

$$\forall \varepsilon \quad \exists n_1 \in \mathbf{N} \quad \forall n > n_1 \quad m > n_1 \quad d(x_n, x_m) < \varepsilon.$$

Une suite pour laquelle cette propriété est vérifiée est dite une *suite de Cauchy* et nous pouvons dire : une suite convergente est une suite de Cauchy.

Mais nous ne savons pas si la réciproque est vraie.

Dans **Q**, cette réciproque est fausse (la suite des valeurs décimales à 10^{-n} près de $\sqrt{2}$ est une suite de Cauchy et ne converge pas). Un espace où cette réciproque est vraie, c'est-à-dire *un espace métrique où toute suite de Cauchy converge, est un espace complet* et **Q** n'est pas complet.

Nous allons chercher à construire des extensions de **Q** qui en fassent :

un treillis conditionnellement complet,
un espace métrique complet.

Les procédés que nous utiliserons s'étendraient, le premier à tout espace ordonné dont on veut faire un treillis complet, le deuxième à tout espace métrique dont on veut faire un espace métrique complet.

La propriété remarquable de **Q** est que, en cherchant à obtenir une des deux propriétés, on obtiendra les deux. Les extensions obtenues par les deux procédés seront, en effet, isomorphes.

Elles n'en partent pas moins, de deux points de vue, totalement distincts que nous examinerons successivement.

§ 2. POINT DE VUE DE L'ORDRE

1. Définition de $\overline{\mathbf{R}}$.

Nous utiliserons une variante des coupures de Dedekind s'appuyant sur la notion de : *section commençante.*

On dit que s est une section commençante d'un ensemble totalement ordonné E si :

$$x \in s \quad y < x \quad \Rightarrow \quad y \in s.$$

Une section finissante, définie de façon analogue, sera le complémentaire d'une section commençante.

Une section commençante peut posséder un plus grand élément ; elle est alors dite *fermée ;* elle peut ne pas en posséder ; elle est alors dite *ouverte.*

Si on considère les rationnels $x \leqslant r$, ils constituent une section commençante fermée.

Si on considère les rationnels $x < r$, ils constituent une section commençante ouverte $s(r)$; mais il suffirait de leur rajouter r pour en faire une section fermée.

Au contraire, l'ensemble des rationnels :

$$\{ r \in \mathbf{Q} ; r^3 < 2 \}$$

est une section commençante ouverte qu'on ne peut pas fermer en lui rajoutant un élément.

Tout rationnel r définit donc une section commençante ouverte et une seule (formée de tous les rationnels $< r$). Mais à certaines sections commençantes ne correspond aucun rationnel ; et l'idée est alors la suivante : nous considérerons *l'ensemble des sections commençantes ouvertes de* **Q**. Nous le nommerons $\overline{\mathbf{R}}$.

$$\overline{\mathbf{R}} \subset \mathcal{P}(\mathbf{Q}).$$

Remarquons d'abord que cet ensemble contient $\emptyset$ et **Q** qui l'un et l'autre satisfont à la définition (on peut les désigner par $-\infty$ et $+\infty$ respectivement).

Examinons les propriétés de $\overline{\mathbf{R}}$.

2. Structure d'ordre de $\overline{\mathbf{R}}$.

D'abord, cet ensemble jouit d'une *structure d'ordre total.* Cet ordre est défini par l'inclusion ; car, si deux sections commençantes s_1 et s_2 sont distinctes, l'une est incluse dans l'autre. Soient en effet :

$$s_1 \neq s_2 \qquad \exists x_1 \in s_1 \qquad x_1 \notin s_2$$

Ces hypothèses entraînent :

$$\forall x_2 \in s_2 \qquad x_2 < x_1 \qquad \text{(définition de } s_2\text{)}$$

d'où :

$$x_2 \in s_1 \qquad \text{(définition de } s_1\text{)}$$

donc :

$$s_2 \subset s_1.$$

Si nous considérons l'ensemble $\tilde{\mathbf{Q}}$ formé des sections commençantes ouvertes, $s(r)$, déterminées par les rationnels, et qui est un sous-ensem-

ble de $\overline{\mathbf{R}}$, nous voyons que l'ordre défini ci-dessus est l'ordre sur $\tilde{\mathbf{Q}}$ défini par l'ordre sur les rationnels.

$$\tilde{\mathbf{Q}} \approx \mathbf{Q}$$

l'isomorphisme indiqué ne concernant, pour le moment, que la structure d'ordre.

Nous allons voir que $\overline{\mathbf{R}}$ *est un treillis complet.*

Observons d'abord qu'une réunion de sections commençantes ouvertes est une section commençante ouverte. Il est évident que c'est une section commençante (qui peut être **Q** tout entier) ; d'autre part, si elle possédait un plus grand élément, il devrait appartenir à une des sections, dont il serait le plus grand élément, ce qui est contraire à l'hypothèse.

Si alors on considère un ensemble de sections $\{s_i\ ;\ i \in I\}$,

$$\sup \{s_i\ ;\ i \in I\} = \bigcup \{s_i\ ;\ i \in I\}$$

D'autre part, on peut énoncer :

Théorème : Si un ensemble ordonné possède un plus petit élément et si tout sous-ensemble de cet ensemble admet une borne supérieure, il admet aussi une borne inférieure.

Démonstration : soit E l'ensemble ordonné et $X \in \mathcal{P}(E)$, et :

$$X^+ = \{y\ ;\quad \forall x \in X \quad x \prec y\}$$

l'ensemble des majorants de X ; l'hypothèse est que sup. X existe, donc que X^+ a un plus petit élément.

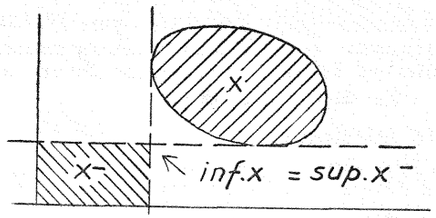
Appelons de même :

$$X^- = \{y\ ;\quad \forall x \in X \quad x \succ y\}$$

l'ensemble des minorants de X. Cet ensemble n'est pas vide puisque nous avons supposé que E avait un plus petit élément. Il s'agit de montrer que X^- a un plus grand élément.

Or, par hypothèse, X^- possède une borne supérieure sup. X^- ; dire que X^- a un plus grand élément est donc équivalent à sup. $X^- \in X^-$. Or, sup. X^- est par définition le plus petit élément de $(X^-)^+$, ensemble des majorants de X^-. Or, $(X^-)^+ \supset X$, donc le plus petit élément de $(X^-)^+$ est un minorant de X, c'est-à-dire sup. $X^- \in X^-$, donc inf. X existe.

(Ci-dessous schéma dans le cas du plan ordonné par la convention : les éléments positifs sont ceux du premier quadrant).



Ce théorème appliqué à $\overline{\mathbf{R}}$ qui possède ø comme le plus petit élément et dont on a déjà montré que tout sous-ensemble avait un sup. prouve que $\overline{\mathbf{R}}$ est un treillis complet.

Exercice 58. — Considérer l'ensemble de toutes les sections commençantes ouvertes ou fermées de **Q**. Montrer que cet ensemble est totalement ordonné et est un treillis complet. Interpréter cet ensemble.

Exercice 59. — Montrer que $\overline{\mathbf{R}}$ est, à un isomorphisme près, le plus petit treillis complet contenant **Q**.

Remarques : Entre deux réels, il y a toujours un rationnel. Soient en effet deux éléments s_1 et s_2 de $\overline{\mathbf{R}}$ tels que $s_1 < s_2$, ce qui veut dire :

$$s_1 \neq s_2 \text{ et } s_1 \subset s_2 \Rightarrow \exists u \in \mathbf{Q} \quad u \in s_2 \quad u \notin s_1,$$

s_2 n'ayant pas de plus grand élément.

$$\exists v > u \qquad v \in s_2.$$

Soient $s(u)$ et $s(v)$ les sections commençantes définies par u et v :

$$s_1 \subset s(u) \subset s(v) \subset s_2$$

De ces trois inclusions, la deuxième est stricte ($u \notin s(u)$, $u \in s(v)$), ainsi que la 3e ($v \notin s(v)$, $v \in s_2$), donc :

$$s_1 \leqslant u < v < s_2$$

(u et v étant maintenant considérés comme éléments de $\tilde{\mathbf{Q}} \subset \overline{\mathbf{R}}$, identifié avec **Q**).

Inversement, entre deux rationnels, il existe toujours un réel non rationnel. Soient en effet deux rationnels a et b ($a < b$). Nous pouvons considérer un réel non rationnel quelconque, $\sqrt{2}$ par exemple, et deux rationnels c et d ($c < d$), faisant respectivement partie de la section commençante qui l'a défini et de son complémentaire. Puis, considérons l'application définie sur **Q** :

$$x \longrightarrow \frac{b-a}{d-c}(x-c) + a$$

homothétie choisie de façon à faire correspondre a à c, b à d, et tous les rationnels de $[a, b]$ à tous les rationnels de $[c, d]$, et par conséquent à la section commençante définissant $\sqrt{2}$, une section sommençante définissant un réel compris entre a et b ; ce réel ne peut être rationnel, car l'application réciproque lui ferait correspondre un rationnel. Il y a donc un réel non rationnel entre a et b.

Ces propriétés s'exprimeront en disant que **Q** *est dense* (*pour l'ordre*) *sur* $\overline{\mathbf{R}}$ et que le complémentaire de **Q** (par rapport à $\overline{\mathbf{R}}$), soit $\overline{\mathbf{R}} - \mathbf{Q}$, *est dense sur* $\overline{\mathbf{R}}$.

3. Définition de R.

La question de l'ordre sur $\overline{\mathbf{R}}$ semble donc réglée, mais nous savons que nous allons rencontrer des difficultés quand nous allons chercher les autres structures de $\overline{\mathbf{R}}$. Nous avons vu en effet qu'un treillis complet ne pouvait pas être un groupe parce qu'un groupe ne pouvait posséder ni plus grand, ni plus petit élément.

Le plus grand et le plus petit éléments de $\overline{\mathbf{R}}$ sont **Q** et ø. Si nous retranchons de $\overline{\mathbf{R}}$ ces deux éléments, nous obtenons un ensemble **R** qui n'est plus un treillis complet mais qui est encore un treillis conditionnellement complet. En effet, si nous considérons un sous-ensemble de **R**

majoré, la réunion des sections commençantes qui définissent ses éléments sera encore une section commençante (qui ne risquera plus d'être **Q** tout entier) et cet ensemble possédera encore un sup. ; enfin, si cet ensemble est minoré, le théorème de la page 86 reste valable et l'ensemble possède encore un inf. ; **R** *est donc un treillis conditionnellement complet.*

Nous allons maintenant rechercher sur **R** la structure de corps, en cherchant comment on peut étendre à **R** les opérations sur **Q**.

4. Structure de groupe commutatif de R.

L'addition sur **R** est définie comme addition sur l'ensemble des parties :

$$s_1 + s_2 = \{ x_1 + x_2 \ ; \ x_1 \in s_1, \ x_2 \in s_2 \} .$$

Il est immédiat que l'opération est associative et commutative. Il est aussi immédiat qu'elle induit l'addition sur **Q**.

Elément neutre : Considérons $s(0)$, c'est-à-dire $\mathbf{Q}^- = \{ 0 \}$.

Nous avons bien pour tout s_1 :

$$s_1 + s(0) \subset s_1,$$

mais réciproquement, soit $x \in s_1$. Il n'y a pas dans s_1 de plus grand élément, donc :

$$\exists y \in s_1 \quad y > x, \quad x - y \in s(0),$$

donc :

$$\forall x \in s_1 \quad x = y + (x - y) \in s_1 + s(0),$$

ce qui permet de conclure que :

$$s_1 + s(0) = s_1,$$

$s(0)$ est bien élément neutre.

Elément symétrique de s_1. Considérons $-s_1$ (au sens de l'opération sur les parties d'un ensemble, c'est-à-dire ensemble des symétriques des éléments de s_1), c'est une section finissante ; $\complement - s_1$ est une section commençante ; cette section peut être fermée par un rationnel ; dans ce cas, on le retire et on considère la section commençante ouverte correspondante que nous désignerons par $\complement^* - s_1$. Etant donné qu'on peut définir :

$$-s_1 = \{ x \ ; \quad \exists u_1 \in s_1 \qquad -u_1 < x \} ,$$

on a :

$$\complement - s_1 = \{ x \ ; \quad \forall u_1 \in s_1 \qquad -u_1 > x \}$$

Donc, si on considère $s_1 + \complement - s_1$ qui est l'ensemble

$$\{ x + u_1 \ ; \ x \in \complement - s_1, u_1 \in s_1 \}$$

avec

$$-u_1 > x, \text{ donc } x + u_1 < 0,$$

on peut affirmer $s_1 + \complement - s_1 \subset s(0)$.

Reste à savoir si, à la place de l'inclusion ci-dessus, on a l'égalité, c'est-à-dire si un nombre négatif quelconque $-q$ appartient à

$$s_1 + \complement - s_1.$$

Ici intervient la propriété du groupe additif des rationnels d'être archimédien. Considérons l'ensemble des nombres nq, $q > 0$, $n \in \mathbf{Z}$.

Puisque s_1 n'est ni $\emptyset$ ni **Q**, il existe $a \in s_1$, $b \in \complement s_1$, et du fait que **Q** est archimédien.

$$\exists n_1, n_2 \in \mathbf{Z} \qquad n_1 q < a \text{ d'où } n_1 q \in s_1$$
$$n_2 q > b \text{ d'où } n_2 q \in \complement s_1$$

Mais, entre $n_1 q$ et $n_2 q$, il y a un nombre fini de multiples de q. Il existe donc n tel que :

$$nq \in s_1 \quad (n+1)\, q \in \complement s_1$$
$$-(n+1)\, q \in -\complement s_1 = \complement - s_1.$$

A ce moment :

$$-q = nq - (n+1)\, q \in s_1 + \complement - s_1,$$

donc :

$$s_1 + \complement - s_1 = s(0)$$

est démontrée. Dans le cas où $\complement - s_1$ n'est pas fermée, elle est la section commençante ouverte inverse de s_1 pour l'addition. Dans le cas contraire, c'est $\complement^* - s_1$ qu'il faut considérer ; il pourrait alors se produire que le rationnel retiré de $\complement - s_1$ soit justement $(n+1)q$. Entre $nq \in s_1$ et $(n+2)q \in \complement^* - s_1$, il y aurait alors une différence de 2 q. Il suffirait de remplacer dans le raisonnement précédent q par $\frac{q}{2}$ pour retrouver une différence de q et prouver ainsi que $-q$ appartient à $s_1 + \complement^* - s_1$.

Nous avons donc démontré que toute section commençante ouverte a un inverse par rapport à l'addition. Remarquons que le raisonnement eût été en défaut si nous avions gardé $\emptyset$ et **Q** parmi les éléments à considérer. D'ailleurs :

$$\forall s_1 \qquad \mathbf{Q} + s_1 = \mathbf{Q}$$
$$\emptyset + s_1 = \emptyset$$

$\emptyset$ et **Q** n'ont donc effectivement pas d'éléments symétriques. Nous retrouvons le fait qu'ils ne pouvaient pas faire partie d'un groupe additif.

Rapprochant la loi de groupe ainsi mise en évidence et la structure d'ordre, nous voyons que **R** *est un groupe ordonné.* En effet,

$$s_1 \subset s_2 \ \Rightarrow \ s_1 + s \subset s_2 + s.$$

Ce groupe est archimédien. Soient en effet a et b deux réels ; nous voulons montrer qu'on peut trouver $n \in \mathbf{N}$ tel que $na > b$. Soit r un rationnel inférieur à a et r' un rationnel supérieur à b ; puisque **Q** est archimédien, il existe n tel que :

$$nr > r'$$
donc : $$na > nr > r' > b.$$

Conséquence : Soit X un sous-ensemble de **R** et x sa borne supérieure

$$\forall \varepsilon \in \mathbf{R}^+ - \{ 0 \} \qquad \exists y \in \mathrm{X} \qquad x - \varepsilon < y \leqslant x.$$

En effet, il existe n tel que :

$$(n-1)\,\varepsilon < x \leqslant n\varepsilon,$$

et puisque x est borne supérieure, il existe y tel que :

$$(n-1)\,\varepsilon < y \leqslant x,$$

sans quoi $(n-1)\,\varepsilon$ serait un majorant de X inférieur à x.

Exercice 60. — 1° Tout groupe totalement ordonné archimédien est isomorphe à un sous-groupe de **R** (et est par conséquent commutatif).

2° Tout groupe totalement ordonné, archimédien, dense pour l'ordre et conditionnellement complet est isomorphe à **R** (dense pour l'ordre veut dire qu'entre deux éléments distincts quelconques il en existe un troisième distinct des précédents).

5. Structure de corps de R.

Multiplication : la définition de l'opération ne peut être donnée de façon immédiate à l'aide d'une opération sur l'ensemble des parties, car le produit de deux sections commençantes ne serait pas une section commençante.

En conséquence, on procède comme suit :

On définit d'abord l'opération sur $\mathbf{R}^+$ seulement de la façon suivante : chaque section commençante $s > s(0)$ est remplacée par

$$s' = s \cap (\mathbf{Q}^+ - \{0\}),$$

c'est-à-dire qu'elle est tronquée et réduite à sa partie strictement positive ; on fait le produit (au sens de produit sur l'ensemble des parties de ces sections tronquées) et on rajoute $\mathbf{Q}^-$ à l'ensemble obtenu.

$$s'_1 s'_2 = \{x_1 x_2 \,;\, x_1 \in s'_1 \quad x_2 \in s'_2\}$$
$$s_1 s_2 = s'_1 s'_2 \cup \mathbf{Q}^-.$$

L'ensemble $s_1 s_2$ est bien une section commençante ouverte. On vérifie que $\mathbf{R}^+$ forme un groupe commutatif par rapport à l'opération ainsi définie.

Cette opération est associative, commutative et distributive par rapport à l'addition sur $\mathbf{R}^+$.

Elle induit la multiplication sur $\mathbf{Q}^+$.

Elément neutre : $s(1)$ est tel que $\forall s \in \mathbf{R}^+$, $s(1)\,s \subset s$, de plus tout élément y de s appartient à $s(1)s$, car :

$$\forall y \in s \quad \exists z \in s \quad y < z \quad \text{donc } \frac{y}{z} < 1$$

et

$$y = \frac{y}{z} \times z \qquad \frac{y}{z} \in s(1) \qquad z \in s$$

donc :

$$s(1)s = s.$$

Elément inverse. Soit $s' = s \cap (\mathbf{Q}^+ - \{0\})$, $\dfrac{1}{s'}$ est une section finissante et son complémentaire (relatif à $\mathbf{Q}^+ - \{0\}$) est une section commençante tronquée qui, si elle possède un plus grand élément, sera remplacée par la section commençante $\complement^{*1}_{s'}$.

On a $s' \complement^{*1}_{s'} \subset s'(1)$ avec $s'(1) = s(1) \cap (\mathbf{Q}^+ - \{0\})$.

Il faut encore voir si cette inclusion peut être remplacée par l'égalité. Remarquons d'abord que :

$$\complement^{*1}_{s'} = \frac{1}{\complement^{*}_{s'}}.$$

Ceci posé, soit $q > 0$ quelconque,

$$\exists u \in s' \quad u + q \notin s' \text{ d'où } \frac{1}{u+q} \in \complement^{*1}_{s'}.$$

$$\frac{u}{u+q} \in s' \complement^{*1}_{s'},$$

$\dfrac{u}{u+q} = 1 - \dfrac{q}{u+q} > 1 - \dfrac{q}{u_0}$, si u_0 est un élément fixe de s', q étant quelconque et u_0 fixe, $1 - \dfrac{q}{u_0}$ est arbitrairement proche de 1 et appartient à $s' \complement^{*1}_{s'}$ qui contient donc $s'(1)$.

Enfin, on étend l'opération à **R** entier en lui imposant d'être distributive par rapport à l'addition sur **R**, ce qui conduit à la règle des signes. **R** est bien alors doté d'une structure de corps.

R *est un corps ordonné.* Nous avons déjà vu que **R** était un groupe additif ordonné. D'autre part, nous venons de voir que le produit de deux éléments de $\mathbf{R}^+$ était un élément de $\mathbf{R}^+$. Donc, **R** est un corps ordonné.

Exercice 61. — Toute application de **R** dans **R** qui vérifie

$$f(x+y) = f(x) + f(y)$$

et qui est croissante est définie par

$$f(x) = \lambda x$$

où λ est un réel fixe.

Que pourrait-on dire de f si la condition « f croissante » était abandonnée ?

6. Limites dans R.

Montrons maintenant que *toute suite de Cauchy converge dans* **R**.

Soit une suite de Cauchy $\{x_n\}$.

Une telle suite est bornée supérieurement :

$$\forall n \in \mathbf{N}. \quad |x_n| < \mathrm{H}$$

Il existe donc des éléments v_p de **R** définis par :

$$v_p = \sup. \{x_n \,;\, n \geqslant p\}$$
$$\forall p \quad |v_p| \leqslant \mathrm{H}$$

$v_{p+1} \leqslant v_p$ puisque v_{p+1} est le sup. d'un ensemble inclus dans le précédent.

Posons $u = \inf. v_p$.

Le fait que u_n soit une suite de Cauchy permet d'écrire :

$$\forall \varepsilon > 0 \qquad \exists n_0 \qquad \forall_m^n \geqslant n_0 \qquad |x_n - x_m| < \varepsilon.$$

La définition de v_p et le fait que v_{p+1} soit inférieur à v_p permettent d'écrire :

$$\forall \varepsilon \qquad \exists n_1 \qquad \forall p > n_1 \qquad \exists u < v_p < u + \varepsilon \qquad \text{d'où } |u - v_p| < \varepsilon.$$

Soit alors n_2, le plus grand des deux nombres n_0 et n_1.

Si p est un nombre supérieur à n_2 :

$$\exists \nu \geqslant p > n_2 \quad v_p - \varepsilon < x_\nu < v_p \text{ d'où } |x_\nu - v_p| < \varepsilon.$$

On peut alors affirmer :

$$\forall n > n_2 \qquad |x_n - u| \leqslant |x_n - x_\nu| + |x_\nu - v_p| + |v_p - u| < 3\varepsilon,$$

3ε étant positif arbitraire, la suite $\{x_n\}$ converge vers u.

Limites supérieure et inférieure d'une suite de réels.

Si $\{ x_n \}$ est une suite de réels bornée quelconque, il existe un élément de **R** défini par :

$$\inf_{n} \sup_{m \geqslant n} x_m.$$

On l'appelle limite supérieure de la suite et on la note :

$$\limsup x_n \quad \text{ou} \quad \overline{\lim}\, x_n.$$

Si la suite n'est pas bornée, cet élément existe encore dans $\overline{\mathbf{R}}$.

Cette définition de la limite supérieure est en général plus maniable que la suivante plus ancienne à laquelle elle est équivalente :

a) $\overline{\lim}\, x_n = +\infty$ veut dire : $\forall a \in \mathbf{R}+ \quad \exists n \quad x_n > a$;

b) $\overline{\lim}\, x_n = -\infty$ veut dire : $\forall a \in \mathbf{R}+ \quad \exists n_0 \quad \forall n > n_0 \quad x_n < -a$;

c) $\overline{\lim}\, x_n = \mathrm{L}$ veut dire : 1) $\forall \varepsilon > 0 \quad \exists n_0 \quad \forall n > n_0 \quad x_n < \mathrm{L} + \varepsilon$ (il n'y a qu'un nombre fini d'éléments de la suite $\geqslant \mathrm{L} + \varepsilon$) ;

2) $\forall \varepsilon > 0 \quad \forall n \quad \exists m > n \quad x_m > \mathrm{L} - \varepsilon$ (il existe une infinité d'éléments de la suite supérieurs à $\mathrm{L} - \varepsilon$).

Exercice 62. — Etablir l'équivalence des deux définitions.
Des remarques analogues peuvent être faites pour

$$\underline{\lim}\, x_n = \sup_{n} \inf_{m \geqslant n} x_m$$

Exercice 63. — Etablir $\underline{\lim}\, x_n \leqslant \overline{\lim}\, x_n$.
Montrer que dans le cas de l'égalité la suite $\{ x_n \}$ a une limite.

Remarque : les définitions ci-dessus sont valables dans un treillis complet où elles permettent de définir la limite d'une suite (égalité de $\overline{\lim}\, x_n$ et $\underline{\lim}\, x_n$), définition qui n'utilise que la structure d'ordre et n'exige pas qu'une distance soit définie sur l'ensemble dans lequel est prise la suite.

En particulier sur $\mathcal{P}(\mathrm{E})$, on peut définir pour toute suite de parties $\{ \mathrm{E}_n \}$:

$$\overline{\lim}\, \mathrm{E}_n = \bigcap_{n \in \mathbf{N}} \bigcup_{m \geqslant n} \mathrm{E}_m$$

$$\underline{\lim}\, \mathrm{E}_n = \bigcup_{n \in \mathbf{N}} \bigcap_{m \geqslant n} \mathrm{E}_m$$

Exercice 64. — Etudier la relation entre $\overline{\lim}\, x_n$ pour $x_n \in \mathbf{R}$ et $\overline{\lim}\, s(x_n)$ où $s(x_n) \in \mathcal{P}(\mathbf{R})$ est la section commençante ouverte déterminée par x_n.

7. Généralisation. Plongement d'un ensemble ordonné dans un treillis complet.

Exercice 65. — Question préliminaire. X et Y étant deux parties d'un ensemble ordonné, montrer que

$$X \subset Y \Rightarrow X+ \supset Y+ \Rightarrow X+- \subset Y+-$$

Soit alors E un ensemble ordonné. On considère l'ensemble

$$T = \{ X^- ; X \in \mathcal{P}(E) \}$$

T est ordonné par l'inclusion sur $\mathcal{P}$ (E).

1. Montrer que T est un treillis complet ; pour cela on montrera :
a) que tout sous-ensemble $\{ X_i^- \}$ de T admet une borne inférieure car

$$\cap X_i^- = (\cup X_i)^-$$

b) que tout sous-ensemble admet une borne supérieure. Il suffira d'appliquer le théorème corrélatif de celui de la page 86 ; on devra distinguer le cas où E possède un plus grand élément ω et celui où E n'en possède pas et montrer que dans les deux cas E est le plus grand élément de T.

2. Montrer que $T \supset \tilde{E}$, $\tilde{E}$ étant un ensemble isomorphe à E pour la structure d'ordre ; pour cela
a) on définira

$$\tilde{E} = \{ a^- ; a \in E \}$$

et on montrera que l'ordre sur T induit sur $\tilde{E}$ l'ordre déduit de celui de E dans la bijection

$$a^- \in \tilde{E} \longleftrightarrow a \in E$$

b) on montrera que dans cette bijection la borne inférieure d'une partie de $\tilde{E}$ est image de la borne inférieure de la partie homologue de E quand celle-ci en possède une dans E ;
c) on montrera la même propriété pour les bornes supérieures.

§ 3. POINT DE VUE METRIQUE. COMPLETION DES RATIONNELS PAR LES SUITES DE CAUCHY.

1. Définition de R.

Notre but est maintenant de plonger les rationnels dans un ensemble plus vaste où toutes les suites de Cauchy seraient convergentes. Suivant en cela une démarche analogue à celle que nous avons suivie pour la complétion pour l'ordre, nous considérerons d'abord dans ce but *l'ensemble dont les éléments sont les suites de Cauchy de* **Q**. Soit $\mathcal{A}$ cet ensemble. L'ensemble des suites définies sur un anneau a une structure d'anneau, car cet ensemble est l'ensemble des applications :

$$\mathbf{N} \to \mathbf{Q} \text{ (considéré comme anneau)}$$

et nous avons vu (exercice 37) que la structure d'anneau de l'ensemble d'arrivée permettait de définir une structure d'anneau sur l'ensemble des applications. Notre ensemble $\mathcal{A}$ est donc une partie de cet anneau et nous allons vérifier que c'est un sous-anneau, donc qu'il *jouit d'une structure d'anneau.*

Soient $\{ x_n \}$ et $\{ y_n \}$ les suites de Cauchy de termes généraux x_n et y_n. Nous poserons :

$$\{ x_n \} + \{ y_n \} = \{ x_n + y_n \}$$
$$\{ x_n \} \{ y_n \} = \{ x_n y_n \}.$$

Il est immédiat que $\{ x_n + y_n \}$ est une suite de Cauchy, car :

$$|(x_n + y_n) - (x_m + y_m)| \leqslant |x_n - x_m| + |y_n - y_m|$$

et $\quad \exists n_0 \quad \forall n, m > n_0 \quad |x_n - x_m| < \varepsilon$

$$\exists n_1 \quad \forall n, m > n_1 \quad |y_n - y_m| < \varepsilon,$$

donc :

$$\forall n, m > \sup(n_1, n_0) \quad |(x_n + y_n) - (x_m + y_m)| < 2\varepsilon.$$

Pour le produit, nous remarquons d'abord *qu'une suite de Cauchy est bornée* car :

$$\forall n, m \geqslant n_0 \quad |x_n - x_m| < \varepsilon$$

entraîne $\quad \forall n > n_0 \quad x_{n_0} - \varepsilon < x_n < x_{n_0} + \varepsilon.$

Donc, pour toute suite de Cauchy,

$$\exists \mathrm{H} \quad \forall n \quad |x_n| < \mathrm{H}.$$

Ceci dit, H et K étant les bornes des 2 suites $\{ x_n \}$ et $\{ y_n \}$, on peut écrire :

$$\forall n, m > \sup(n_1, n_0) \qquad |x_n y_n - x_m y_m| \leqslant |x_n|\,|y_n - y_m| + |y_m|\,|x_n - x_m| \leqslant H\varepsilon + K\varepsilon.$$

L'existence de l'élément nul et des éléments opposés est évidente :

$$0 = \{ 0 \} \qquad -\{ x_n \} = \{ -x_n \}.$$

Les opérations sont associatives.

Enfin, la multiplication est distributive par rapport à l'addition.

$\mathcal{A}$ est donc un anneau. Il a un élément unité :

$$1 = \{ 1 \}.$$

Mais $\mathcal{A}$ est trop grand pour notre propos. En effet, nous cherchons un ensemble qui contienne **Q** ou du moins un ensemble isomorphe à **Q**. Or, il existe une infinité de suites de Cauchy qui convergent vers un rationnel donné ξ. Il y a d'abord la suite $\{ \xi \}$ dont tous les termes sont égaux à ξ, mais il y a aussi toutes les suites :

$$\{ x_n \} = \{ \xi + \varepsilon_n \},$$

ε_n tendant vers zéro quand n tend vers l'infini (et il y a seulement celles-là). Il y a donc une infinité de suites qui correspondent à un même rationnel et il convient de les regrouper, c'est-à-dire de regrouper toutes les suites dont la différence est une suite qui converge vers zéro.

L'ensemble des suites qui convergent vers zéro est un idéal J, puisque la différence de deux telles suites et le produit d'une telle suite par une suite de Cauchy (donc bornée) quelconque sont encore des suites qui convergent vers 0.

Deux suites qui convergent vers le même rationnel sont deux suites qui appartiennent à la même classe de $\mathcal{A}$ mod J. Cela nous amène donc à prendre comme nouvel ensemble **R** *l'anneau quotient* $\mathcal{A}/J$, ensemble dans lequel un seul élément correspond à un rationnel.

2. Structure algébrique de R.

$\mathcal{A}$ étant un anneau commutatif et unitaire, nous aurons prouvé que $\mathcal{A}/J$ est un corps si nous prouvons que J est maximal (voir III. 4, 4).

Soit donc à étudier l'idéal $J + \{ x_n \}$ où $\{ x_n \}$ désigne une suite de Cauchy qui ne tend pas vers zéro. La suite $\left\{\frac{1}{x_n}\right\}$ ne peut être considérée directement, car certains des termes de $\{ x_n \}$ pourraient être nuls. Mais le terme général d'une suite de Cauchy qui ne converge pas vers zéro reste à partir d'un certain rang de valeur absolue supérieure à un nombre fixe (et de signe constant). En effet, la définition d'une suite de Cauchy appartenant à J étant :

$$\forall \varepsilon \quad \exists n_0 \qquad \forall n > n_0 \qquad |x_n| < \varepsilon$$

celle d'une suite n'appartenant pas à J est :

$$\exists \varepsilon \quad \forall n_0 \qquad \exists n_1 > n_0 \qquad |x_{n_1}| \geqslant \varepsilon \qquad (1).$$

Ecrivons alors :

$$x_{n_1} = x_n + x_{n_1} - x_n$$
$$|x_{n_1}| \leqslant |x_n| + |x_{n_1} - x_n|$$
$$|x_n| \geqslant |x_{n_1}| - |x_{n_1} - x_n|$$

$\{ x_n \}$ étant une suite de Cauchy,

$$\exists n_2 \qquad \forall n, n_1 > n_2 \quad |x_{n_1} - x_n| < \frac{\varepsilon}{2} \qquad (2).$$

Prenons alors $n_0 = n_2$. La ligne (1) nous affirme l'existence de $n_1 > n_2$ tel que $|x_{n_1}| > \varepsilon$ et la ligne (2) que pour tout $n > n_2$:

$$|x_{n_1} - x_n| < \frac{\varepsilon}{2}.$$

Il en résulte que :

$$\forall n > n_2 \qquad |x_n| > \frac{\varepsilon}{2}$$

Remarque : L'inégalité (2) qui peut s'écrire, étant donné $n_1 > n_2$:

$$\forall n > n_2 \qquad x_{n_1} - \frac{\varepsilon}{2} < x_n < x_{n_1} + \frac{\varepsilon}{2},$$

alors que $|x_{n_1}| > \varepsilon$, prouve en outre que x_n est du signe de x_{n_1}, donc d'un signe constant à partir d'un certain rang.

Ceci dit, considérons la suite $\{ y_n \}$ ainsi définie :

$$\forall n > n_2 \quad y_n = x_n \qquad \forall n \leqslant n_2 \quad y_n = 1.$$

Il est clair que $\{ y_n - x_n \} \in J$,

c'est-à-dire que $\{ y_n \} \in J + \{ x_n \}$.

Or, considérons la suite $\left\{\frac{1}{y_n}\right\}$. Si n et m sont supérieurs à n_2,

$$\left|\frac{1}{y_n} - \frac{1}{y_m}\right| = \frac{|x_n - x_m|}{|x_n|\,|x_m|} < |x_n - x_m| \times \frac{4}{\varepsilon^2},$$

où ε est le nombre fixe précédemment déterminé.

$\{ x_n \}$ étant une suite de Cauchy,

$$\forall \eta \qquad \exists n_0 \qquad \forall n, m > n_0 \qquad |y_n - y_m| < \eta$$

puisqu'il suffira d'avoir $|x_m - x_n| < \eta \frac{\varepsilon^2}{4}$.

$\left\{\frac{1}{y_n}\right\}$ est donc une suite de Cauchy.

$\{ y_n \} \times \left\{\frac{1}{y_n}\right\} = \{ 1 \}$ appartient alors à l'idéal $J + \{ x_n \}$.

Contenant $\{ 1 \}$, cet idéal contient l'anneau tout entier. Donc, J *est maximal et* $\mathcal{A}/J = \mathbf{R}$ *est un corps.*

Revenons au sous-ensemble :

$$\tilde{\mathbf{Q}} \subset \mathcal{A}/J$$

formé des classes de suites de Cauchy qui convergent vers un rationnel ; un élément de cet ensemble est la classe $\tilde{\xi}$ formée de toutes les suites de Cauchy qui convergent vers le rationnel ξ. La bijection :

$$\tilde{\xi} \in \tilde{\mathbf{Q}} \longleftrightarrow \xi \in \mathbf{Q}$$

est évidemment un isomorphisme puisqu'il suffit de penser aux suites constantes $\{ \xi \}$ et $\{ \eta \}$ appartenant aux classes $\tilde{\xi}$ et $\tilde{\eta}$ pour voir que :

$$\tilde{\xi} + \tilde{\eta} = \widetilde{\xi + \eta}$$
$$\tilde{\xi} \times \tilde{\eta} = \widetilde{\xi\eta}.$$

Q *est donc isomorphe au sous-corps* $\tilde{\mathbf{Q}}$ *de* **R**.

3. Structure d'ordre.

Montrons d'abord que **R** est un corps ordonné. Il faut trouver un $\mathbf{R}^+$ pour l'addition (voir propriétés des G^+ : II, 4, 1).

Puisque nous avons vu qu'à partir d'un certain rang tous les termes d'une suite de Cauchy n'appartenant pas à J ont un signe déterminé et puisqu'il est évident que les éléments d'une même classe mod J, sauf ceux de J, sont ainsi des suites dont tous les éléments sont positifs ou dont tous les éléments sont négatifs (à partir d'un certain rang), on pourra prendre comme $\mathbf{R}^+$ l'ensemble des classes dont les éléments sont des suites à termes positifs (à partir d'un certain rang), ensemble auquel on ajoutera J. Cet ensemble est tel que :

$$\mathbf{R}^+ + \mathbf{R}^+ = \mathbf{R}^+ \quad \text{et} \quad \mathbf{R}^+ \cap \mathbf{R}^- = \{ 0 \},$$

puisque les seules suites appartenant aux classes de $\mathbf{R}^+$ et à celles de son opposé sont celles de J. En outre, $\mathbf{R} = \mathbf{R}^+ \cup \mathbf{R}^-$. $\mathbf{R}$ jouit donc d'une structure d'ordre total compatible avec l'addition.

D'autre part, $\mathbf{R}^+ \times \mathbf{R}^+ \subset \mathbf{R}^+$. Donc (voir note IV, 1), $\mathbf{R}$ *est un corps totalement ordonné.*

$\mathbf{Q}$ *est dense pour l'ordre sur* $\mathbf{R}$, c'est-à-dire qu'entre deux éléments de $\mathbf{R}$ il y a toujours un élément de Q. Soient, en effet :

$$x \in \mathbf{R} \qquad y \in \mathbf{R} \qquad x < y$$

et soient $\{ a_n \}$ et $\{ b_n \}$ deux suites de Cauchy appartenant respectivement aux classes d'équivalence définissant x et y.

$$\{ b_n - a_n \} \notin \mathrm{J} \qquad \text{classe de } \{ b_n - a_n \} \in \mathbf{R}^+$$

Donc : $\exists h \qquad \exists n_0 \qquad \forall n > n_0 \qquad |b_n - a_n| > h.$

D'autre part, puisque $\{ a_n \}$ et $\{ b_n \}$ sont des suites de Cauchy,

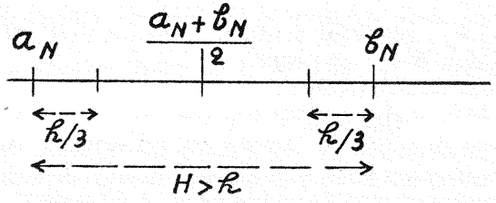
$$\forall \varepsilon \qquad \exists n_1 \qquad \forall n, m > n_1 \qquad |b_n - b_m| < \varepsilon \qquad |a_n - a_m| < \varepsilon.$$

Nous pourrons choisir $\varepsilon = \dfrac{h}{3}$. Soit alors un nombre fixe :

$$\mathrm{N} > \sup \{ n_0, n_1 \} \qquad b_{\mathrm{N}} - a_{\mathrm{N}} = \mathrm{H} > h$$

$$\forall n > \mathrm{N} \qquad |b_{\mathrm{N}} - b_n| < \frac{h}{3} \quad \text{ce qui implique} \quad b_n > b_{\mathrm{N}} - \frac{h}{3}$$

$$|a_{\mathrm{N}} - a_n| < \frac{h}{3} \quad \text{ce qui implique} \quad a_n > a_{\mathrm{N}} + \frac{h}{3}$$



D'où, si nous considérons la moyenne de a_{N} et de b_{N}, on peut affirmer :

$$\forall n > \mathrm{N} \qquad a_n < \frac{a_{\mathrm{N}} + b_{\mathrm{N}}}{2} < b_n \qquad (1).$$

Si nous prenons alors la suite constante :

$$\{ \mathrm{V}_n \} = \left\{ \frac{a_{\mathrm{N}} + b_{\mathrm{N}}}{2} \right\}$$

cette suite appartient à $\tilde{\mathbf{Q}}$ puisque $\dfrac{a_{\mathrm{N}} + b_{\mathrm{N}}}{2}$ est rationnel, et (1) entraîne :

$$x < \text{classe } \{ \mathrm{V}_n \} < \mathrm{y}.$$

De même, le complément de $\mathbf{Q}$ est dense sur $\mathbf{R}$, pour l'ordre (rien

à changer à la démonstration donnée avec l'autre mode de construction de $\mathbf{R}$).

L'ordre sur $\mathbf{R}$ est *archimédien.* Cela résulte de ce que $\mathbf{Q}$ est archimédien et de ce qu'étant donné $x \in \mathbf{R}$, $y \in \mathbf{R}^+ - \{ 0 \}$, on pourra toujours trouver :

$$a \in \mathbf{Q} \quad \text{et} \quad a > x$$
$$\text{et } b \in \mathbf{Q} \qquad 0 < b < y$$

ce qui donnera :

$$\exists n \in \mathbf{N} \qquad ny > nb > a > x.$$

4. Propriétés métriques de Q.

Distance sur $\mathbf{R}$: La distance de deux éléments x et y de $\mathbf{R}$ est :

$$|x - y|$$

au sens de la définition donnée de ce symbole pour les groupes ordonnés (voir II, 4, 2), qui pour un groupe totalement ordonné équivaut à :

$$|x - y| = x - y \qquad \text{si } x > y,$$
$$= y - x \qquad \text{si } x < y.$$

Il est immédiat que l'application de $\mathbf{R} \times \mathbf{R}$ dans $\mathbf{R}^+$ ainsi définie est bien une distance puisque :

$$|x - y| = 0 \Rightarrow x = y$$
$$|x - y| = |y - x|$$

et qu'enfin l'inégalité triangulaire est vérifiée comme nous l'avons montré (exercice 31).

Or, si x est défini par la classe de la suite de Cauchy $\{ x_n \}$ et y par la classe de la suite de Cauchy $\{ y_n \}$, $x - y$ et $y - x$ sont respectivement les classes de $\{ x_n - y_n \}$ et $\{ y_n - x_n \}$. Or si $x \neq y$, par exemple, pour fixer les idées, si $x > y$, la suite $\{ x_n - y_n \} \notin \mathrm{J}$ et, à partir d'un certain rang, $x_n - y_n$ est positif. Donc, $|x - y|$ qui, dans le cas où nous nous sommes placés, est $x - y$, est défini par la suite dont le terme général est toujours $x_n - y_n$. Dans le cas contraire, elle le serait par celle de terme général $y_n - x_n$. Donc, dans tous les cas :

$$|x - y| = \text{ classe de } \{ |x_n - y_n| \}.$$

Cette règle appliquée à deux éléments $\tilde{\xi}$ et $\tilde{\eta}$ de Q donne :

$$|\tilde{\xi} - \tilde{\eta}| = \text{classe de } \{ |\xi - \eta| \} = \widetilde{|\xi - \eta|}.$$

L'isomorphisme

$$\tilde{\mathbf{Q}} \longleftrightarrow \mathbf{Q}$$

s'étend donc à la distance. (Un élément de $\tilde{\mathbf{Q}}$ et son homologue dans $\mathbf{Q}$ ont des distances homologues dans l'isomorphisme).

$\tilde{\mathbf{Q}}$ *est dense sur* $\mathbf{R}$ *au sens métrique.* Nous entendons par là que :

$$\forall x \in \mathbf{R} \qquad \forall \varepsilon \qquad \exists\, \tilde{\xi} \in \tilde{\mathbf{Q}} \qquad |\tilde{\xi} - x| < \varepsilon.$$

(Contrairement à ce qu'il en était jusqu'ici dans ce chapitre, ε pourra être un réel et non plus seulement un rationnel).

Soit en effet $\{ x_n \}$ une des suites de Cauchy qui définissent x. On peut dire :

$$\forall \varepsilon \in \mathbf{R}^+ \qquad \exists n_0 \qquad \forall n, m > n_0 \qquad |x_n - x_m| < \varepsilon.$$

En effet, d'après ce que nous venons de voir :

$$\exists \varepsilon' \in \tilde{\mathbf{Q}} \quad 0 < \varepsilon' < \varepsilon \quad \text{et} \quad |x_n - x_m| < \varepsilon' \Rightarrow |x_n - x_m| < \varepsilon.$$

Soit alors $\tilde{\xi} \in \tilde{\mathbf{Q}}$ la classe de la suite de Cauchy constante dont le terme général vaut x_p (p étant un entier fixe supérieur à n_0),

$$|x_n - x_p| < \varepsilon \qquad \forall n > n_0$$

et comme :

$$|x - \tilde{\xi}| = \text{classe de } \{ |x_n - x_p| \}$$
$$|x - \tilde{\xi}| < \varepsilon$$

R *est complet, c'est-à-dire que, dans* **R**, *toutes les suites de Cauchy convergent.*

Soit $\{ X_n \}$ une suite de Cauchy de **R**.

$$\forall \varepsilon \quad \exists n_0 \quad \forall n, m > n_0 \quad |X_n - X_m| < \varepsilon.$$

On veut montrer qu'il existe X vers lequel converge la suite. D'après ce qu'on vient de voir, à chaque X_n, on peut faire correspondre $\tilde{\xi}_n \in \tilde{\mathbf{Q}}$ tel que :

$$|X_n - \tilde{\xi}_n| < \frac{1}{2^n}$$

$\tilde{\xi}_n$ est la classe de toutes les suites qui convergent vers ξ_n et, en particulier, celle de la suite constante dont tous les termes valent ξ_n.

Soit alors la suite $\{ \xi_p \}$; c'est une suite de Cauchy, en effet :

$$\widetilde{|\xi_n - \xi_m|} = |\tilde{\xi}_n - \tilde{\xi}_m|$$

$$|\tilde{\xi}_n - \tilde{\xi}_m| \leqslant |\tilde{\xi}_n - X_n| + |X_n - X_m| + |X_m - \tilde{\xi}_m|$$

et par suite :

$$\forall \varepsilon > 0 \quad \exists n_0 \quad \forall n, m > n_0 \quad |X_n - X_m| < \frac{\varepsilon}{3}$$

$$\forall \varepsilon > 0 \quad \exists n_1 \quad \forall n > n_1 \quad \frac{1}{2^n} < \frac{\varepsilon}{3}.$$

D'où, en prenant $n_2 = \sup(n_0, n_1)$:

$$\forall n, m > n_2 \quad |\xi_n - \xi_m| < \varepsilon.$$

ξ_p est donc une suite de Cauchy. Soit X sa classe. Nous allons montrer que $\{ X_n \}$ converge vers X.

$$|X_n - X| \leqslant |X_n - \tilde{\xi}_n| + |\tilde{\xi}_n - X|.$$

Nous savons que :

$$\forall n > n_1 \quad |X_n - \tilde{\xi}_n| < \frac{\varepsilon}{3}$$

D'autre part, X est justement la classe de la suite $\{ \xi_p \}$ et par conséquent :

$$|X - \tilde{\xi}_n| = \{ |\xi_p - \xi_n| \} \qquad p \text{ décrivant N}$$

et : $\forall p, n > n_2 \quad |\xi_p - \xi_n| < \varepsilon$

Donc : $\forall n > n_2 \quad |X_n - X| < \frac{4\varepsilon}{3}$ (*).

5. R est un treillis conditionnellement complet.

En effet, soit $X \subset \mathbf{R}$ un ensemble majoré.

Considérons les rationnels de la forme :

$$\frac{p}{2^n}$$

n étant un entier positif fixe et $p \in \mathbf{Z}$.

(*) On obtiendrait un exposé qui serait peut-être plus intuitif en identifiant $\tilde{\mathbf{Q}}$ avec $\mathbf{Q}$ avant de commencer cette démonstration. Nous croyons qu'il est plus instructif, et en un sens aussi plus correct, de ne pas procéder à cette identification. La peine que l'on se sera donnée aboutira en définitive à plus de clarté et de rigueur dans la conception de l'espace complété.

R étant archimédien, il existe un nombre p_1 tel que $\frac{p_1}{2^n}$ soit un majorant de X et un nombre $p_2 < p_1$ tel que $\frac{p_2}{2^n}$ ne soit pas un majorant de X. Dans l'ensemble fini des nombres $\frac{p}{2^n}$ avec $p_2 < p \leqslant p_1$, il existe donc un plus petit nombre qui soit majorant de X ; soit $\frac{p_0(n)}{2^n}$ ce nombre, $\frac{p_0(n) - 1}{2^n}$ n'est pas majorant. Entre ces deux nombres, il existe au moins un élément de X. La moyenne des deux nombres précédents est un nombre de la forme $\frac{p'}{2^{n+1}}$. Ou bien lui, ou bien $\frac{p_0(n)}{2^n}$ est le plus petit majorant de cette forme. Notons celui qui l'est :

$$\frac{p_0(n+1)}{2^{n+1}}$$

On aura :

$$\frac{p_0(n) - 1}{2^n} < \frac{p_0(n+1)}{2^{n+1}} \leqslant \frac{p_0(n)}{2^n}$$

Entre les deux premiers des nombres ci-dessus, il y a au moins un élément de X et nous pouvons recommencer l'opération précédente. Nous définissons ainsi la suite :

$$\{ x_n \} = \left\{ \frac{p_0(n)}{2^n} \right\}$$

qui est non croissante et qui est une suite de Cauchy puisque :

$$\forall m > n \quad |x_m - x_n| < \frac{1}{2^n}.$$

Cette suite de Cauchy converge donc vers un nombre S qui est un majorant, car, s'il n'en était pas un, il y aurait au moins un élément de X supérieur à S et, entre S et cet élément, on trouverait des éléments de la suite, ce qui est absurde. D'autre part, la suite des nombres :

$$\{ y_n \} = \left\{ \frac{p_0(n) - 1}{2^n} \right\}$$

est pour la même raison que $\{ x_n \}$ une suite convergente et, puisque $y_n - x_n$ tend vers 0, elles convergent vers le même nombre. S'il existait un majorant de X inférieur à S, il devrait donc exister des éléments de $\{ y_n \}$ entre ce majorant et X, ce qui est absurde. S est donc inférieur à tous les majorants. C'est donc la borne supérieure de X. Un raisonnement analogue établirait l'existence d'une borne inférieure pour tout X minoré. **R** est donc bien un treillis conditionnellement complet.

6. Equivalence des deux définitions.

R défini comme nous venons de le faire s'avère donc être un groupe totalement ordonné, archimédien, dense pour l'ordre et treillis conditionnellement complet. Il suffit alors de se reporter à l'exercice 60 pour voir que **R** tel que nous venons de le définir est isomorphe à **R** tel qu'il a été défini en le complétant pour l'ordre. Nous identifierons dorénavant les deux ensembles ainsi définis.

7. Généralisation. Complétion d'un espace métrique.

Exercice 66. — Soit E un espace métrique sur lequel est définie une distance à valeurs dans $\mathbf{R}+$. Considérons l'ensemble $\mathcal{C}$ des suites de Cauchy de E.

On désigne par $x = \{ x_n \}$, $y = \{ y_n \}$, ...les éléments de $\mathcal{C}$ et on considère sur $\mathcal{C}$ la relation d'équivalence $xRy \Longleftrightarrow \lim_n d(x_n, y_n) = 0$. On considère enfin l'ensemble $\mathcal{C}/_R = \widehat{E}$ dont on désigne les éléments par $\dot{x}$, $\dot{y}$,... ($\dot{x}$ désignant la classe d'équivalence de x).

1) a) Montrer l'existence de $\lim_n d(x_n, y_n)$.

b) Posant $d(x, y) = \lim_n d(x_n, y_n)$, montrer que $d(x, y)$ ne dépend que des classes des éléments x et y.

c) Posant alors $d(x, y) = d(\dot{x}, \dot{y})$, montrer qu'on obtient une distance sur $\widehat{E}$.

2) On trouvera dans $\widehat{E}$ un ensemble $\dot{E} \subset \widehat{E}$ isométrique à E c'est-à-dire tel qu'il existe une bijection

$$\dot{E} \longleftrightarrow E$$

conservant la distance (la distance de deux éléments est la même que celle de leurs homologues).

3) On prouvera :

a) que $\dot{E}$ est dense sur $\widehat{E}$,

b) que $\widehat{E}$ est complet, c'est-à-dire que toutes les suites de Cauchy y convergent.

4) Les propriétés 3° a) et b) caractérisent $\widehat{E}$ à une isométrie près.

Exemples : Un disque ouvert du plan est un espace métrique pour la distance euclidienne. En le complétant, on obtient un ensemble isométrique au disque fermé.

Si E est l'ensemble des fonctions continues sur [0, 1], on peut y définir deux distances importantes, à savoir :

$$d_1 = \int_0^1 |f(t) - g(t)|\, dt$$

et :

$$d_2 = \sqrt{\int_0^1 [f(t) - g(t)]^2\, dt}.$$

E n'est pas complet pour ces distances. Quand on le complète par rapport à l'une ou l'autre, on obtient deux espaces différents utilisés en analyse (espaces L_1 et L_2).

SOLUTION DES EXERCICES

Exercice 1.

Pour constituer un sous-ensemble on devra devant chacun des n éléments répondre par oui ou par non à la question : « Cet élément fera-t-il partie du sous-ensemble ? » Il y a donc deux possibilités pour le premier élément, 2×2 pour l'ensemble des deux premiers..., etc..., 2^n pour l'ensemble des n éléments donc $N = 2^n$ sous-ensembles possibles.

Une autre solution consiste à considérer l'ensemble des parties comme la réunion des ensembles formés par les combinaisons des n objets p à p, p prenant toutes les valeurs possibles de 0 à n. D'où :

$$N = 1 + C_n^1 + \ldots\ldots + C_n^p + \ldots\ldots + C_n^n = (1 + 1)^n = 2^n.$$

Exercice 2.

Ces deux égalités se vérifient aisément sur des schémas. Elles se démontrent aussi en remarquant que chacun des trois membres représente la réunion des deux ensembles (disjoints) :

$$\{ x ; x \in A, x \notin B \} \text{ et } \{ x ; x \notin A, x \in B \}.$$

Exercice 3.

$(A \Delta B) \Delta C$ est la réunion des deux ensembles :

$(A \Delta B) - C = \{ x ; x \in A, x \notin B, x \notin C$ ou $x \notin A, x \in B, x \notin C \}$

et $C - (A \Delta B) = \{ x ; x \in C, x \in \complement\, A \Delta B \}$.

Or, le complémentaire de $A \Delta B$ est la réunion des deux ensembles :

$$\{ x ; x \notin A, x \notin B \} \text{ et } \{ x ; x \in A, x \in B \}.$$

En définitive $(A \Delta B) \Delta C$ est la réunion des quatre ensembles (deux à deux disjoints) :

$$\{ x ; x \in A, x \notin B, x \notin C \}$$
$$\{ x ; x \notin A, x \in B, x \notin C \}$$
$$\{ x ; x \notin A, x \notin B, x \in C \}$$
$$\{ x ; x \in A, x \in B, x \in C \}$$

donc des ensembles formés des éléments qui appartiennent à un seul des trois ensembles A, B, C, ou aux trois à la fois. La forme même du résultat qui est indépendante de l'ordre dans lequel on considère les ensembles démontre la propriété *d'associativité* de la différence symétrique.

Cette opération admet pour *élément neutre* l'ensemble vide :

$$A \Delta \emptyset = A.$$

D'autre part :

$$A \Delta A = \emptyset.$$

L'ensemble des parties forme donc par rapport à la différence symétrique un groupe commutatif où chaque élément est son propre inverse.

Exercice 4.

a) $$A \Delta B = (A - B) \cup (B - A).$$

Or, d'après la définition, $A - B \in \mathcal{F}$, $B - A \in \mathcal{F}$, donc leur réunion appartient à $\mathcal{F}$. De même l'intersection :

$$A \cap B = (A \cup B) - (A \Delta B),$$

différence de deux ensembles appartenant à $\mathcal{F}$ appartient à $\mathcal{F}$. Réciproquement, si on considère une famille $\mathcal{F}'$ tel que :

$$A, B \in \mathcal{F}' \Rightarrow A \Delta B \in \mathcal{F}', \quad A \cap B \in \mathcal{F}',$$

on peut dire :

$$A - B = \{ x \,;\, x \in A, x \notin B \} = (A \Delta B) \cap A$$

donc $$A - B \in \mathcal{F}'.$$

D'autre part, observons que pour deux ensembles disjoints leur différence symétrique est leur réunion. Et appliquons ceci aux deux ensembles $A \Delta B$ et $A \cap B$:

$$(A \Delta B) \Delta (A \cap B) = (A \Delta B) \cup (A \cap B) = A \cup B,$$

donc $$A \cup B \in \mathcal{F}'.$$

Montrer que $\mathcal{F}$ a pour ces deux opérations une structure d'anneau commutatif se réduit à montrer que l'intersection est distributive par rapport à la différence symétrique (il est facile de voir que l'inverse est faux).

Comparons donc :

$$(A \Delta B) \cap C \text{ et } (A \cap C) \Delta (B \cap C).$$

On vérifiera que ces deux ensembles sont formés de la réunion des deux ensembles disjoints :

$$\{ x \,;\, x \in A, x \notin B, x \in C \}$$
$$\{ x \,;\, x \notin A, x \in B, x \in C \}$$

b) Montrons d'abord que la réunion d'un nombre fini de semi-segments ouverts à droite est la réunion d'un nombre fini de tels semi-segments deux à deux disjoints.

Soient $a_i \leqslant x < a'_i$ ces semi-segments et soit a_0 le plus petit de tous les a_i ; considérons tous les semi-segments tels que $a_i < a'_0$, soit a'_1 le plus grand de tous les a'_i ; la réunion de tous ces semi-segments est le semi-segment $a_0 \leqslant x < a'_1$. Considérons alors tous les semi-segments tels que $a_i < a'_1$ et soit a'_2 le plus grand de tous leurs a'_i ; la réunion de tous les semi-segments considérés jusqu'à maintenant est le semi-segment $a_0 \leqslant x < a'_2$ et ainsi de suite... Ce processus s'arrête nécessairement au bout d'un nombre fini d'opérations en remplaçant la réunion d'un certain nombre de semi-segments par un seul semi-segment $a_0 \leqslant x < a'_n$. Soit alors b_0 le plus petit des $a_i > a'_n$. On recommence à partir de lui le même raisonnement et on trouve un nouveau semi-segment $b_0 \leqslant x < b_p$ disjoint du premier. Si le processus n'a pas épuisé les semi-segments on recommence une 3e fois à partir du plus petit des $a_i > b_p$ et ainsi de suite.

Soit alors la famille dont chaque élément est une réunion finie de semi-segments d'une même droite. La réunion de deux tels éléments est encore une réunion finie de semi-segments et appartient à la famille. Le raisonnement précédent montre que cette famille est identique à celle des réunions finies de semi-segments deux à deux disjoints. Pour montrer que cette famille est une famille $\mathcal{F}$ il reste donc seulement à montrer que la différence $E - F$ de deux éléments appartient à la famille.

Mais, E étant formé de semi-segments deux à deux disjoints :

$$E - F = \bigcup \{ [a_i, a'_i[- F \}$$

$[a_i, a'_i[$ désignant le semi-segment $a_i \leqslant x < a'_i$.

D'autre part F étant aussi formé de semi-segments $[b_j, b'_j[$ disjoints il est clair que :

$$[a_i, a'_i[- F = [a_i, a'_i[- [b_1, b'_1[- [b_2, b'_2[- \ldots, \text{ etc...}$$

c'est-à-dire que l'on retire successivement de $[a_i, a'_i[$ tous les points appartenant aux semi-segments de F. Il reste donc seulement à voir ce qu'est la différence de deux semi-segments ; quatre cas de figure se présentent et suivant les cas on voit que la différence est, soit un semi-segment, soit la réunion de deux semi-segments disjoints, soit l'ensemble vide. La différence $[a_i, a'_i[- F$ est donc une réunion de semi-segments deux à deux disjoints et $E - F$ l'est aussi.

Il est facile de vérifier que cette propriété relative à la différence serait fausse pour des segments $[a, a']$ ainsi que pour des intervalles ouverts $]a, a'[$.

Exercice 5.

Le graphe est constitué de deux réseaux de points de l'angle *xoy* (déterminé par les directions positives de deux axes), l'un formé de tous les points dont les coordonnées sont paires, l'autre de tous les points de coordonnées impaires.

Exercice 6.

Il existe une bijection évidente de l'ensemble des applications de $E - A$ dans F sur l'ensemble des extensions de f à E. Or $\mathcal{F}(E - A, F)$ est fini si et seulement si on se trouve dans l'un des deux cas suivants : *a*) F n'a qu'un élément (il n'existe alors qu'une extension) ; *b*) F et $E - A$ sont finis. (Si n et p sont leurs nombres respectifs d'éléments, il existe p^n extensions distinctes).

Exercice 7.

Soient E, F, G les trois ensembles et les applications dans lesquelles ils se correspondent :

$$E \underset{g}{\overset{f}{\rightarrow}} F \overset{i}{\rightarrow} G$$

i étant injective tout élément de G correspond à un seul élément de F, donc :

$$\forall x \quad i \circ f(x) = i \circ g(x) \Rightarrow f(x) = g(x)$$

donc :

$$f = g.$$

Réciproquement, si une application i est telle que la relation (sur $\mathcal{F}(E, F)$, ensemble des applications de E dans F) définie par :

$$i \circ f = i \circ g \qquad (1)$$

soit l'identité, c'est-à-dire si :

$$\forall f, g \qquad i \circ f = i \circ g \Rightarrow f = g$$

on peut affirmer que i est injective.

En effet, considérons les applications f_a et f_b qui à tout $x \in E$ font correspondre respectivement l'élément fixe a et l'élément fixe b de F (applications constantes). L'hypothèse appliquée à ces applications donne :

$$i \circ f_a = i \circ f_b \Rightarrow f_a = f_b, \text{ c'est-à-dire } a = b.$$

Or, $\forall x \in E \quad i \circ f_a(x) = i(a) \quad i \circ f_b(x) = i(b).$

L'hypothèse s'écrit donc :

$$i(a) = i(b) \Rightarrow a = b$$

autrement dit : i est injective.

Observons que cette démonstration n'a pas utilisé la totalité de l'hypothèse, mais seulement le fait que la relation (1) est vérifiée par les applications constantes de E dans F. L'énoncé de la réciproque pourrait être modifié en conséquence.

Soient encore :

$$E \xrightarrow{s} F \underset{g}{\xrightarrow{f}} G$$

L'hypothèse est que $\forall x \in E \qquad f \circ s(x) = g \circ s(x)$
mais s étant surjective, $s(x)$ décrit tout F ; donc :

$$\forall y = s(x) \in F \qquad f(y) = g(y).$$

Réciproquement, si $f \circ s = g \circ s \Rightarrow f = g$ quelles que soient f et g, s est surjective.

En effet, si s n'était pas surjective on pourrait considérer un élément y_0 de F n'appartenant pas à $s(E)$ et deux applications f et g telles que :

$$\forall y \in s(E) \qquad f(y) = g(y) \text{ et } f(y_0) \neq g(y_0).$$

Pour deux telles applications on aurait $f \circ s = g \circ s$ sans avoir $f = g$, ce qui est contraire à l'hypothèse.

Exercice 8.

1) $f(A \cup B)$ est l'ensemble des y qui sont images d'au moins un élément ou de A, ou de B, donc qui appartiennent à $f(A)$ ou $f(B)$ (« ou » n'étant pas exclusif), c'est-à-dire à $f(A) \cup f(B)$.

Inversement, un élément de $f(A) \cup f(B)$ est l'image d'un élément qui appartient à A ou à B, donc à $A \cup B$. On peut donc écrire :

$$f(A \cup B) = f(A) \cup f(B).$$

2) $f(A \cap B)$ est l'ensemble des images des x qui appartiennent à A et à B ; donc ces images appartiennent à $f(A)$ et $f(B)$ à la fois, ce qui entraîne :

$$f(A \cap B) \subset f(A) \cap f(B).$$

Mais un élément de $f(A) \cap f(B)$ est l'image d'au moins un élément de A et d'au moins un élément de B qui peuvent être distincts. Ils ne peuvent l'être si f est injective et dans ce cas l'élément dont l'image appartient à $f(A) \cap f(B)$ appartient à $A \cap B$.

Donc *si f est injective,* $f(A \cap B) = f(A) \cap f(B)$.

3) $f(\complement A)$ est l'ensemble des images des x qui n'appartiennent pas à A :

$$f(\complement A) = \{ y \,;\, y = f(x) \quad x \notin A \}.$$

Mais si f n'est pas injective, un x appartenant à A peut avoir même image qu'un x appartenant à $\complement A$; d'autre part si f n'est pas surjective des points de $\complement f(A)$ peuvent n'appartenir ni à $f(\complement A)$ ni à $f(A)$. Aucune propriété simple n'apparaît donc en général. Mais il résulte du raisonnement précédent que :

si f est injective	$f(\complement A) \subset \complement f(A)$
si f est surjective	$f(\complement A) \supset \complement f(A)$
si f est bijective	$f(\complement A) = \complement f(A)$

Exercice 9.

L'existence de g telle que $g \circ f = I_E$ montre que tout élément de F obtenu par f, c'est-à-dire appartenant à $f(E)$, est l'image d'un élément unique de E, sans quoi (g étant une application) $g \circ f$ ne donnerait qu'une image de plusieurs éléments et ne serait pas l'identité. Nous pouvons donc déjà dire que *l'existence de g satisfaisant à la première égalité prouve que f est injective.*

D'autre part si la seconde égalité est vérifiée, à tout élément de F, g fait correspondre un élément de E et $f \circ g$ fait correspondre lui-même. C'est donc que $f(E)$ décrit tout F, autrement dit que f est surjective. *L'existence de g satisfaisant à la deuxième égalité prouve que f est surjective.*

L'existence de g satisfaisant aux deux égalités prouve que f est bijective.

Exercice 10.

On peut écrire :

$$\overset{-1}{f}(A \cap B) = \{ x \,;\, f(x) \in A,\ f(x) \in B \}$$

or :

$$f(x) \in A \text{ signifie } x \in \overset{-1}{f}(A)$$

$$f(x) \in B \text{ signifie } x \in \overset{-1}{f}(B)$$

donc l'ensemble précédent peut s'écrire :

$$\begin{aligned} \overset{-1}{f}(A \cap B) &= \{ x \,;\, x \in \overset{-1}{f}(A),\ x \in \overset{-1}{f}(B) \} \\ &= \{ x \,;\, x \in \overset{-1}{f}(A) \cap \overset{-1}{f}(B) \} \\ &= \overset{-1}{f}(A) \cap \overset{-1}{f}(B). \end{aligned}$$

De même :

$$\begin{aligned} \overset{-1}{f}(A \cup B) &= \{ x \,;\, f(x) \in A \text{ ou } f(x) \in B \} \\ &= \{ x \,;\, x \in \overset{-1}{f}(A) \text{ ou } x \in \overset{-1}{f}(B) \} \\ &= \{ x \,;\, x \in \overset{-1}{f}(A) \cup \overset{-1}{f}(B) \} \\ &= \overset{-1}{f}(A) \cup \overset{-1}{f}(B). \end{aligned}$$

Et enfin :

$$\begin{aligned} \overset{-1}{f}(\complement_F A) &= \{ x \,;\, f(x) \notin A \} = \{ x \,;\, x \notin \overset{-1}{f}(A) \} \\ &= \{ x \,;\, x \in \complement_E \overset{-1}{f}(A) \} = \complement_E \overset{-1}{f}(A). \end{aligned}$$

Exercice 11.

Soient deux ensembles E et F et soit A une partie de E. Examinons :

$$\overset{-1}{f} \circ f(A).$$

Tous les éléments de $B = f(A)$ sont images d'un élément de A, mais si f n'est pas injective ils peuvent être en même temps image d'autres éléments de E, donc :

$$\overset{-1}{f} \circ f(A) \supset A$$

et *si f est injective :*

$$\overset{-1}{f} \circ f(A) = A.$$

Soit maintenant A une partie de F. Examinons :

$$f \circ \overset{-1}{f}(A).$$

$B = \overset{-1}{f}(A)$ représente l'ensemble des $x \in E$ qui ont leur image dans A ; l'application f transforme ces éléments en éléments de A, mais si f n'est pas surjective des éléments de A pourraient ne pas avoir d'image réciproque appartenant à B, donc :

$$f \circ \overset{-1}{f}(A) \subset A$$

et *si* B *est surjective :*

$$f \circ \overset{1}{f}(A) = A.$$

Exercice 12.

$$\bigcup \{ A ; A \in \mathcal{F} \} \cup \bigcup \{ B ; B \in \mathcal{G} \}$$

représente l'ensemble des x tels qu'il existe au moins une partie A appartenant soit à $\mathcal{F}$, soit à $\mathcal{G}$, c'est-à-dire appartenant à $\mathcal{F} \cup \mathcal{G}$ dont x soit élément ; c'est donc :

$$\bigcup \{ A ; A \in \mathcal{F} \cup \mathcal{G} \}.$$

De même :

$$\bigcup \{ A ; A \in \mathcal{F} \} \cap \bigcup \{ B ; B \in \mathcal{G} \}$$

est l'ensemble des x tels qu'il existe à la fois une partie $A \in \mathcal{F}$ et une partie $B \in \mathcal{G}$ dont x soit élément ; c'est-à-dire qu'il existe un couple A, B, autrement dit un élément du produit cartésien $\mathcal{F} \times \mathcal{G}$ tel que $x \in A \cap B$. On peut donc écrire :

$$\bigcup \{ A ; A \in \mathcal{F} \} \cap \bigcup \{ B ; B \in \mathcal{G} \} = \bigcup \{ A \cap B ; (A, B) \in \mathcal{F} \times \mathcal{G} \}.$$

Les formules duales sont respectivement :

$$\bigcap \{ A ; A \in \mathcal{F} \} \cap \bigcap \{ B ; B \in \mathcal{G} \} = \bigcap \{ A ; A \in \mathcal{F} \cup \mathcal{G} \}$$

et :

$$\bigcap \{ A ; A \in \mathcal{F} \} \cup \bigcap \{ B ; B \in \mathcal{G} \} = \bigcap \{ A \cup B ; (A, B) \in \mathcal{F} \times \mathcal{G} \}.$$

On peut aussi les établir directement.

Le premier membre de la première représente l'ensemble des x qui appartiennent à tous les $A \in \mathcal{F}$ et à tous les $B \in \mathcal{G}$, donc à tous les éléments de $\mathcal{F} \cup \mathcal{G}$, ce qui démontre la formule. Le premier membre de la deuxième représente l'ensemble des x qui appartiennent soit à tous les $A \in \mathcal{F}$, soit à tous les $B \in \mathcal{G}$; un tel x appartient donc à $A \cup B$ pour tout couple $(A, B) \in \mathcal{F} \times \mathcal{G}$. Montrons que réciproquement tout x de l'ensemble du 2e membre fait partie de l'ensemble du premier membre. S'il appartient à $\bigcap \{ A ; A \in \mathcal{F} \}$ la propriété est démontrée ; sinon, c'est qu'il existe au moins un A, soit $A_0 \in \mathcal{F}$, tel que $x \notin A_0$. Mais alors pour que x appartienne à tous les $A \cup B$, ce qui implique, en particulier :

$$\forall B \in \mathcal{G} \qquad x \in A_0 \cup B$$

il est nécessaire que :

$$\forall B \in \mathcal{G} \qquad x \in B$$

donc :

$$x \in \bigcap \{ B ; B \in \mathcal{G} \}$$

et la propriété est encore démontrée.

Exercice 13.

a) Comparons :

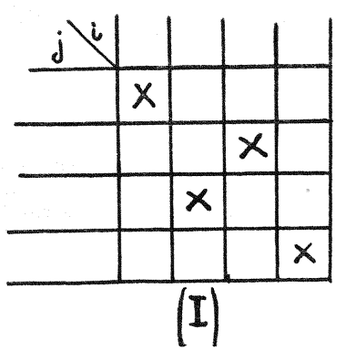
$$A = \bigcup_i \left(\bigcap_j X_{ij} \right) \text{ et } B = \bigcap_j \left(\bigcup_i X_{ij} \right).$$

On peut écrire :

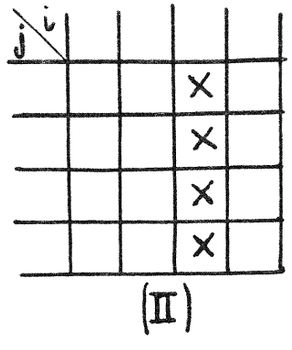
$$x \in A \iff \exists i \quad \forall j \qquad x \in X_{ij}$$
$$x \in B \iff \forall j \quad \exists i \qquad x \in X_{ij}.$$

Il est clair que :

$$A \subset B.$$



(I)



(II)

En effet, mettons les X_{ij} dans un tableau à double entrée et cochons les X_{ij} qui admettent un x donné pour élément. Pour que x appartienne à B il faut et il suffit qu'une case soit cochée dans chaque ligne (graphique I). Pour que x appartienne à A il faut en outre que toutes ces cases appartiennent à une même colonne (graphique II). Donc :

$$x \in A \Rightarrow x \in B.$$

b) On peut dire que x appartient à B si, et seulement si, il existe une application :

$$j \to i = f(j)$$

(application dont le graphe est représenté schématiquement par I) telle que :

$$\forall j \quad x \in X_{f(j),j}$$

donc telle que :

$$x \in \bigcap_j X_{f(j),j}$$

On peut donc écrire :

$$x \in B \iff \exists f \in \mathcal{F}(J, I) \quad x \in \bigcap_j X_{f(j),j}$$

$\mathcal{F}$ désignant l'ensemble des applications de J dans I.

Donc :

$$B = \bigcup_{f \in \mathcal{F}} \bigcap_j X_{f(j),j}.$$

Par dualité on trouve :

$$A = \bigcap_{f \in \mathcal{F}} \bigcup_j X_{f(j),j}.$$

Exercice 14.

S étant une relation d'équivalence, on a $f(x)Sf(x)$, ce qui entraîne xRx ; R est réflexive.

D'autre part :

$$xRy \Rightarrow f(x)Sf(y) \Rightarrow f(y)Sf(x) \text{ puisque S est symétrique}$$

et $f(y)Sf(x) \Rightarrow yRx$; R est symétrique.

Enfin :

$$xRy,\ yRz \Rightarrow f(x)Sf(y),\ f(y)Sf(z) \Rightarrow f(x)Sf(z)$$

puisque S est transitive ; et $f(x)Sf(z) \Rightarrow xRz$; R est donc transitive.

Exercice 15.

1° La réflexivité $R_1 \prec R_1$ est évidente.

2° $R_1 \prec R_2$ signifie $xR_1y \Rightarrow xR_2y$

$R_2 \prec R_3$ signifie $xR_2y \Rightarrow xR_3y$

donc $R_1 \prec R_2$, $R_2 \prec R_3$ implique que $xR_1y \Rightarrow xR_3y$, c'est-à-dire $R_1 \prec R_3$, la relation $\prec$ est donc transitive.

3° Enfin $R_1 \prec R_2$ et $R_2 \prec R_1$ signifie que $xR_1y \Longleftrightarrow xR_2y$, donc $R_1 = R_2$. La relation est donc antisymétrique. C'est une relation d'ordre. Notons qu'elle équivaut à l'inclusion du graphe de R_1 dans celui de R_2.

Exercice 16.

f_1 et f_2 étant deux applications de E dans F et $\prec$ la relation d'ordre dans F, nous pouvons poser :

$$f_1 \text{ antérieure à } f_2 \Longleftrightarrow \quad \forall x \in E \quad f_1(x) \prec f_2(x).$$

Le fait que les axiomes de la relation d'ordre sont vérifiés est évident.

Exercice 17.

Montrer que $\mathcal{R}$ forme un treillis pour la relation d'ordre indiquée dans l'exercice ci-dessus (n° 15) revient à montrer qu'étant données deux relations d'équivalence R_1 et R_2 on peut trouver une relation R_0 moins fine que toutes les relations plus fines que R_1 et R_2 et une relation S_0 plus fine que toutes les relations moins fines que R_1 et R_2. Or toutes les relations R plus fines que R_1 et R_2 sont telles que :

$$xRy \Rightarrow xR_1y \text{ et } xR_2y.$$

Il en résulte que la relation R_0 définie par :

$$xR_0y \Longleftrightarrow xR_1y \text{ et } xR_2y,$$

dont on vérifie immédiatement qu'elle est réflexive, symétrique et transitive, est entraînée par toutes les relations R et est donc moins fine qu'elles. On peut donc poser :

$$\inf(R_1R_2) = R_0$$

R_0 étant définie comme il vient d'être indiqué et son graphe étant l'intersection des deux graphes R_1 et R_2.

On pourrait être tenté de définir de même S_0 comme la relation dont le graphe est la réunion des deux graphes de R_1 et de R_2, c'est-à-dire prendre pour relation S_0 :

$$xR_1y \text{ ou } xR_2y$$

mais il apparaît que si une relation ainsi définie serait bien réflexive et symétrique elle ne serait pas transitive puisque, étant donnés x, y, z trois éléments de E, on pourrait avoir xR_1y et yR_2z, ce qui n'entraînerait, en général, ni xR_1z ni xR_2z.

Ceci nous amène à définir comme suit la relation S_0 : x et y seront dans la même classe si on peut passer de l'un à l'autre par une suite finie

d'éléments $x, a_1, a_2, ..., a_n, y$ tels que deux éléments consécutifs soient équivalents mod R_1 ou mod R_2 :

$$xS_0y \Longleftrightarrow \exists\, a_1, a_2, ..., a_n \quad \begin{array}{l} xR_1a_1 \text{ ou } xR_2a_1 \\ a_1R_1a_2 \text{ ou } a_1R_2a_2 \\ \dots\dots\dots\dots\dots\dots \\ a_nR_1y \text{ ou } a_nR_2y. \end{array}$$

Cette fois la transitivité est évidente puisqu'il suffira de mettre à la file la chaîne allant de x à y et celle allant de y à z pour avoir une chaîne allant de x à z.

Le graphe de cette relation S_0 inclut la réunion des graphes, mais ne lui est pas identique.

Il reste à montrer qu'elle est plus fine que toutes les autres relations S moins fines que R_1 et R_2.

Une telle relation S est telle que :

$$xR_1y \Rightarrow xSy$$
$$xR_2y \Rightarrow xSy.$$

On aura montré que $S_0 \prec S$ si on montre que :

$$xS_0y \Rightarrow xSy.$$

Or la définition de S_0 entraîne :

$$xS_0y \Rightarrow \left\{ \begin{array}{l} xR_1a_1 \text{ ou } xR_2a_1 \Rightarrow xSa_1 \\ a_1R_1a_2 \text{ ou } a_1R_2a_2 \Rightarrow a_1Sa_2 \\ \dots\dots\dots\dots\dots\dots \\ a_nR_1y \text{ ou } a_nR_2y \Rightarrow a_nSy \end{array} \right\} \Rightarrow xSy$$

On peut donc conclure :

$$\sup(R_1R_2) = S_0.$$

Exercice 18.

Les hypothèses se traduisent par :

$$\dot{x} = \{\, y\ ;\ xRy,\ yRx \,\}$$
$$\dot{x}' = \{\, y'\ ;\ x'Ry',\ y'Rx' \,\}.$$

Nous poserons :

$$\dot{x} \prec \dot{x}' \Longleftrightarrow \quad \exists y \in \dot{x}, \quad \exists y' \in \dot{x}' \qquad yRy'.$$

Montrons qu'il s'agit bien d'une relation d'ordre.

1° Elle est réflexive. En effet : $xRx \Rightarrow \dot{x} \prec \dot{x}$.

2° Elle est transitive. Soit en effet :

$$\dot{x} \prec \dot{x}' \qquad \dot{x}' \prec \dot{x}''.$$

Ces hypothèses entraînent l'existence de :

$$y \in \dot{x},\ y'_1 \in \dot{x}',\ y'_2 \in \dot{x}',\ y'' \in \dot{x}''$$

tels que :

$$yRy'_1 \qquad y'_2Ry''$$

mais y'_1 et y'_2 appartenant à la même classe, on a aussi :

$$y'_1Ry'_2$$

et de la transitivité de R on déduit en rapprochant ces trois relations :

$$yRy'' \text{ donc } \dot{x} \prec \dot{x}''.$$

3° Enfin, elle est antisymétrique. En effet :

$$\dot{x} \prec \dot{x}' \qquad \dot{x}' \prec \dot{x}$$

entraînent l'existence de $y_1 \in \dot{x},\ y_2 \in \dot{x},\ y'_1 \in \dot{x}',\ y'_2 \in \dot{x}'$ tels que :

$$y_1Ry'_1 \qquad y'_2Ry_2\ ;$$

or, la définition de $\dot{x}$ entraîne $y_2 R y_1$, celle de $\dot{x}'$ entraîne $y'_1 R y'_2$. Rapprochons deux à deux ces relations :

$$y_1 R y'_1,\ y'_1 R y'_2 \Rightarrow y_1 R y'_2$$
$$y'_2 R y_2,\ y_2 R y_1 \Rightarrow y'_2 R y_1,$$

ces deux dernières formules expriment que y_1 et y'_2 appartiennent à la même classe, ce qui implique que $\dot{x}$ et $\dot{x}'$ sont confondues.

Remarques :

a) $\dot{x} \prec \dot{x}' \quad \Rightarrow \quad \forall y \in \dot{x} \quad \forall y' \in \dot{x}' \quad y R y'$.

b) La relation R est en quelque sorte une relation d'ordre imparfaite, parfois appelée de « préordre ». On pourrait prendre comme exemples :

1° Sur N, b étant un nombre fixe :

$xRy \iff$ quotient (à 1 près) de x par $b \leqslant$ quotient (à 1 près) de y par b.

Dans une même classe, on a tous les nombres qui ont même quotient et la relation d'ordre sur l'ensemble quotient qu'on peut identifier à l'ensemble des quotients est l'ordre naturel des entiers.

2° Sur un ensemble de mots, R pourra être un ordre lexicographique imparfait ne portant que sur la première lettre du mot. L'ensemble quotient est formé des 26 classes correspondant aux 26 lettres, et ordonné par l'ordre normal des lettres de l'alphabet.

Exercice 19.

Pour trouver toutes les structures possibles de groupe ayant un nombre donné d'éléments, nous devons construire les tables de Pythagore de ces groupes en respectant les principes suivants :

1) Chaque élément figure une fois et une seule dans chaque ligne et chaque colonne (condition que l'on exprime parfois en disant que la table doit être un carré latin).

2) Tout inverse à droite étant inverse à gauche, e doit occuper des places symétriques par rapport à la diagonale principale du carré.

3) L'opération doit être associative.

Pratiquement, on place d'abord e, c'est-à-dire qu'on décide du choix des éléments qui seront inverses les uns des autres ; puis, on place les autres éléments en jouant de l'associativité et en complétant les lignes et les colonnes de façon à vérifier la propriété du carré latin ; enfin on vérifie celles des relations d'associativité qui n'ont pas servi dans la construction.

$n = 3$. Soient e, a, b les trois éléments. On voit tout de suite que si a et b étaient leurs propres inverses, on ne disposerait d'aucune valeur à attribuer à ab. On trouve donc le seul tableau ci-contre.

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Tous les groupes du 3e ordre sont isomorphes les uns aux autres.

$n = 4$. On peut partir *à priori* des deux possibilités suivantes : chaque élément est son propre inverse ou bien un seul élément autre que e est son propre inverse, les deux autres étant inverses l'un de l'autre, ce qui se traduit par les deux tableaux incomplets suivants :

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b			e
c	c		e	

Il est facile de voir qu'à partir de là tout est déterminé et qu'on obtient les deux tableaux suivants :

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Quant à l'associativité de l'opération définie par l'un ou l'autre de ces tableaux, nous nous dispenserons de la vérifier en reconnaissant dans la structure des deux groupes abstraits précédents celle de deux groupes bien connus : pour le premier, celui des symétries par rapport à trois axes formant un trièdre trirectangle (e = transformation identique) ; pour le deuxième, celui des entiers additifs modulo 4 (a = classe des nombres congrus à 2 mod 4).

$n = 5$. Nous pouvons cette fois essayer *à priori* les trois cas suivants : chaque élément est son propre inverse ; trois seulement des éléments sont leur propre inverse ; seul e est son propre inverse. Avec un peu de patience on trouve que les deux premiers cas conduisent à des contradictions et que le troisième cas ne conduit qu'à une seule structure possible. Tous les groupes du 5e ordre sont isomorphes entre eux et isomorphes au groupe additif des entiers modulo 5 (avec $a \equiv 3$, $b \equiv 2$, $c \equiv 1$, $d \equiv 4$).

	e	a	b	c	d
e	e	a	b	c	d
a	a	c	e	d	b
b	b	e	d	a	c
c	c	d	a	b	e
d	d	b	c	e	a

Remarquons que nous n'avons trouvé jusqu'à maintenant que des groupes commutatifs. Il n'existe donc pas de groupe non commutatif à moins de six éléments.

$n = 6$. En raisonnant de façon analogue on trouve trois structures possibles.

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	d	c	e	f	a
c	c	f	e	$\underline{b}$	a	$\underline{d}$
d	d	b	f	a	c	e
f	f	c	a	$\underline{d}$	e	b

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

Dans ces trois structures on peut reconnaître :

pour la première, celle des entiers additifs modulo 6 ;

pour la deuxième, celle des entiers multiplicatifs modulo 7 (avec $e \equiv 1$, $a \equiv 6$, $b \equiv 4$, $c \equiv 2$, $d \equiv 3$, $f \equiv 5$) ;

pour la troisième, le groupe des permutations de trois objets ou, ce qui revient au même, le groupe des isométries conservant un triangle équilatéral (b et a sont les deux rotations d'angle $\pm \frac{2\pi}{3}$; c, d, f, les trois symétries par rapport aux axes du triangle). Ce dernier groupe n'est pas commutatif.

Il est à remarquer que dans une recherche systématique on trouve

des tableaux satisfaisant aux autres propriétés d'une table de groupe mais non associatifs. C'est le cas de celui qu'on obtient en échangeant b et d aux quatre endroits où ils sont soulignés dans le deuxième des tableaux ci-dessus. (On a alors, par exemple, en effet : $c^2 = d$, $bc = e$, donc $(bc)c = c$ et $bc^2 = bd = f$).

Exercice 20.

Dire que l'application

$$a \to \varphi_a$$

est injective c'est dire que :

$$\forall (a, b) \in G^2 \quad b \neq a \Rightarrow \varphi_a \neq \varphi_b,$$

or $\varphi_a \neq \varphi_b$ veut dire :

$$\exists x \quad axa^{-1} \neq bxb^{-1}.$$

Cette dernière propriété est équivalente à la suivante obtenue en multipliant à gauche par b et à droite par a :

$$\exists x \quad b^{-1}ax \neq xb^{-1}a,$$

$\varphi_a \neq \varphi_b$ veut donc dire : il existe un x qui ne commute pas avec $b^{-1}a$. L'élément $b^{-1}a$ ne commute donc pas avec tous les autres; comme il décrit tout $G - \{ e \}$, quand a et b décrivent G en restant différents, dire que φ est injective veut donc dire qu'il n'existe aucun élément, autre que e, qui commute avec tous les autres. φ est donc un isomorphisme si et seulement si G ne possède aucun élément qui commute avec tous les autres.

Exercice 21.

1) Soient $c_1 \in C$, $c_2 \in C$. On peut écrire :

$\forall x \in G \quad x(c_1c_2) = (xc_1)\, c_2 = c_2\,(xc_1) = c_2(c_1x) = (c_2c_1)\, x = (c_1c_2)x$,

en utilisant tantôt l'associativité, tantôt le fait que c_1 ou c_2 commute avec tout élément. On conclut de cette égalité : $c_1c_2 \in C$. D'autre part : $e \in C$.

Enfin,

$\forall x \in G \quad xc_1^{-1} = (c_1x^{-1})^{-1} = (x^{-1}c_1)^{-1} = c_1^{-1}x$,

en utilisant la loi de formation de l'inverse d'un produit, donc $c_1^{-1} \in C$.

Donc, C est un sous-groupe de G.

Ce sous-groupe est invariant car $ac_1a^{-1} = c_1aa^{-1} = c_1$.

2) En nous reportant à l'exercice précédent nous voyons que :

$$\varphi_a = \varphi_b \iff \forall x \quad axa^{-1} = bxb^{-1} \iff b^{-1}a \in C,$$

donc $\varphi_a = \varphi_b$ si et seulement si a et b appartiennent à une même classe de G/C. C'est dire que l'ensemble A des automorphismes intérieurs φ est isomorphe à G/C.

Exercice 22.

1) La relation R définit les classes d'équivalence :

$$\dot{x} = \{ u \,;\, xRu \} \quad \text{et} \quad \dot{y} = \{ v \,;\, yRv \}.$$

Dire qu'on peut définir une loi de composition sur G/R de telle sorte que G/R soit image homomorphe de G, c'est dire que :

$$\forall u \in \dot{x}, \quad \forall v \in \dot{y} \quad xy\, R\, uv.$$

Supposons que R soit régulière :

$$\left.\begin{array}{l} xRu \Rightarrow xy\, R\, uy \\ yRv \Rightarrow uy\, R\, uv \end{array}\right\} \Rightarrow xy\, R\, uv \text{ puisque R est transitive.}$$

Réciproquement si :

$$\forall (u, v) \in G^2 \quad xRu,\ yRv \ \Rightarrow\ xy\, R\, uv,$$

on peut en déduire que R est régulière. En effet :

aRa puisque R est réflexive et

$$\forall a \in G \quad xRu,\ aRa \left\{\begin{array}{l} \Rightarrow x\, a\, R\, u\, a \\ \Rightarrow a\, x\, R\, a\, u \end{array}\right.$$

2) Considérons alors l'élément neutre de l'opération sur G/R, c'est-à-dire la classe de e :

$$\dot{e} = \{ u \,;\, eRu \}.$$

Cette classe forme un sous-groupe de G car eRu, $eRu' \Rightarrow eRuu'$ puisque R est régulière et, pour la même raison, $eRu \Rightarrow eu^{-1}Ruu^{-1}$ donc $u^{-1}Re$; donc le produit de deux de ses éléments et l'inverse d'un de ses éléments appartiennent à $\dot{e}$.

Ce sous-groupe est invariant car la régularité de R permet d'écrire :

$$eRu \Rightarrow a\, e\, a^{-1}\, R\, a\, u\, a^{-1} \Rightarrow e\, R\, a\, u\, a^{-1},$$

c'est-à-dire : $a\,\dot{e}\,a^{-1} = \dot{e}$.

Enfin :

$$xRy \iff xy^{-1}\, Re \iff xy^{-1} \in \dot{e}.$$

En définitive :

R régulière $\Rightarrow$ R de la forme $xy^{-1} \in \dot{e}$ ($\dot{e}$ sous-groupe invariant).

Réciproquement, soit une relation de la forme :

$$xRy \iff xy^{-1} \in g \ (g \text{ sous-groupe invariant}).$$

On a démontré dans le cours que cette relation R était une relation d'équivalence. Il reste donc seulement à montrer qu'elle est régulière, c'est-à-dire que :

$$\forall a \in G \qquad xRy \ \Rightarrow\ ax\, R\, ay \quad \text{et} \quad xa\, R\, ya$$

Or,

$xRy \iff xy^{-1} \in g$ et, puisque g est invariant,

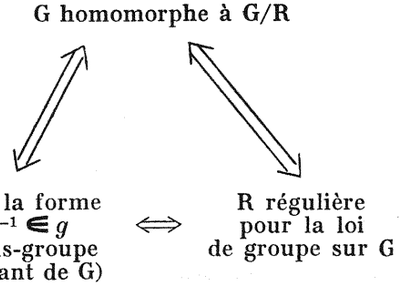
$axy^{-1}a^{-1} \in g$ c'est-à-dire $ax(ay)^{-1} \in g$, soit $ax\, R\, ay$.

D'autre part $xy^{-1} \in g$ peut s'écrire :

$$xaa^{-1}y^{-1} \in g \Rightarrow xa(ya)^{-1} \in g \Rightarrow xa\, R\, ya.$$

(Remarquons que cette deuxième partie du résultat n'a pas utilisé l'hypothèse de l'invariance de g. Nous pourrons donc démontrer que la relation $xy^{-1} \in g$ est une relation d'équivalence régulière à droite pour un sous-groupe quelconque g).

En définitive, cette théorie des homomorphismes des groupes a considéré trois propriétés équivalentes. Dans le cours, on a démontré l'équivalence de gauche ; dans la première question du présent exercice, celle de droite ; dans la deuxième question, celle d'en bas.



Exercice 23.

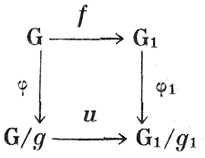
Considérons le diagramme :

$$G \xrightarrow{f} G_1 \xrightarrow{\varphi_1} G_1/g_1$$
$$a \longrightarrow a_1 \longrightarrow \dot{a}_1 = a_1 g_1.$$

L'application $\varphi_1 \circ f$ qui est la composée de deux applications qui sont toutes deux des homomorphismes est par conséquent un homomorphisme. Le groupe G_1/g_1 image homomorphe de G par cette application est donc, d'après le théorème général sur les homomorphismes de groupes, isomorphe à un groupe quotient de G par un sous-groupe invariant qui est l'image réciproque dans G de l'élément neutre de G_1/g_1. Or, cet élément neutre de G_1/g_1 a pour image réciproque par φ_1 dans G_1 le sous-groupe g_1, lequel a pour image réciproque dans G $\overset{-1}{f}(g_1) = g$. g est donc le noyau de l'homomorphisme de G sur G_1/g_1, ce qui démontre que g est un sous-groupe invariant et qu'il existe un isomorphisme u de G/g sur G_1/g_1, tel que :

$$\varphi_1 \circ f = u \circ \varphi$$

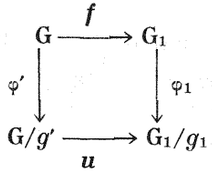
égalité qui exprime que le diagramme suivant est commutatif :



b) Rien n'est changé au début du raisonnement mais le noyau de l'homomorphisme de G sur G_1/g_1 qui est encore $\overset{-1}{f}(g_1)$ est un sous-groupe invariant g' de G tel que :

$$g' = \overset{-1}{f}(g_1) \supset g$$

et on a l'isomorphisme $G/g' \xrightarrow{u} G_1/g_1$
et le diagramme commutatif :



Revenons maintenant à g et examinons alors les deux partitions de G modulo g et modulo g'.

$$\forall a \in G \qquad ag' \supset ag.$$

A une classe ag on peut donc faire correspondre d'une manière unique la classe ag' qui la contient. On pourra donc considérer l'application

$$G/g \xrightarrow{\psi} G/g'$$
$$ag \longrightarrow ag'$$

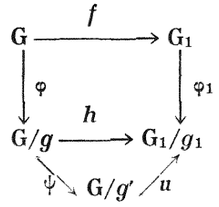
Montrons que cette application est un homorphisme de G/g dans G/g' :

$$\psi(ag.bg) = \psi(abg) = abg' = ag'.bg' = \psi(ag)\psi(bg),$$

φ' se factorise alors :

$$\varphi' = \psi \circ \varphi$$

et nous pouvons préciser le diagramme précédent :



$u \circ \psi = h$ est un homomorphisme de G/g sur G_1/g_1 qui donne le diagramme commutatif prévu par l'énoncé.

Nous pouvons d'ailleurs préciser la relation entre les structures de G/g et G/g'. En appliquant une nouvelle fois le théorème général : G/g' image homomorphe de G/g est isomorphe au groupe quotient de G/g par rapport au noyau de ψ, c'est-à-dire par rapport à l'image réciproque de l'élément unité de G/g'. Cet élément unité est g'. Son image réciproque est l'ensemble des classes modulo g que ψ a envoyées sur g', c'est-à-dire l'ensemble des classes modulo g contenues dans g' ; g étant un sous-groupe invariant de g', cet ensemble des classes modulo g incluses dans g' est le groupe quotient g'/g. On peut donc conclure que :

$$G/g' \approx G/g \,/\, g'/g.$$

Exercice 24.

a) Posons :

$$g' = \complement_G g$$

g, g' constitue une partition de G. Les classes à gauche relatives à g sont g et g' ; les classes à droite g et g'. Donc g est invariant.

b) g_1 et g_2 n'ayant qu'un élément en commun $g_1 \cup g_2$ a $2n - 1$ éléments et il reste un seul élément a tel que :

$$a \in G \qquad a \notin g_1 \qquad a \notin g_2.$$

Soit alors :

$$e \neq x_1 \in g_1 \text{ et considérons le produit :}$$
$$x_1 g_2 = \{ x_1 x_2 \,;\, x_2 \in g_2 \}.$$

Cet ensemble a n éléments parmi lesquels x_1 lui-même. Les $n-1$ autres éléments ne peuvent appartenir ni à g_2 (car $x_1 \notin g_2$), ni à g_1 (car $x_2 \notin g_1$ quand $x_2 \neq e$). Pour les $n-1$ autres éléments qui doivent être distincts, seule la valeur a est possible. Il faut donc que $n-1=1$ et *le seul groupe* G *répondant aux conditions de l'énoncé est donc d'ordre 4.* Ses sous-groupes g_1 et g_2 ne possèdent qu'un élément différent respectivement de x_1 et x_2 ; la loi de groupe est entièrement déterminée par le fait que g_1 est sous-groupe ($x_1^2 = e$), que g_2 est sous-groupe ($x_2^2 = e$), et par le raisonnement fait ci-dessus qui donne $x_1x_2 = a$ et donnerait de même $x_2x_1 = a$. Sur le tableau ci-dessous qui en résulte, on constate que l'ensemble $\{e, a\}$ constitue un 3e sous-groupe invariant.

	e	x_1	x_2	a
e	e	x_1	x_2	a
x_1	x_1	e	a	x_2
x_2	x_2	a	e	x_1
a	a	x_2	x_1	e

c) Soit $g = g_1 \cap g_2$; g constitue un sous-groupe invariant de g_1, de g_2 et de G. Soit p son ordre. Soient alors les groupes quotients G/g, g_1/g et g_2/g ; ce sont respectivement les ensembles de classes :

$$\{ag\ ;\ a \in G\} \qquad \{ag\ ;\ a \in g_1\} \qquad \{ag\ ;\ a \in g_2\}.$$

Il en résulte que :

$$g_1/g \subset G/g \qquad g_2/g \subset G/g.$$

g_1/g et g_2/g sont des sous-groupes d'ordre n/p de G/g qui est d'ordre $2n/p$. D'autre part :

$$g_1/g \cap g_2/g = \{g\}$$

$\{g\}$ désignant la classe de e modulo g, c'est-à-dire l'élément neutre des trois groupes quotients. On est donc ramené au cas précédent. On peut en déduire que $n/p = 2 \qquad 2n = 4p$.

Tout groupe G *d'ordre 2n qui possède deux sous-groupes distincts d'ordre n a un ordre multiple de 4.*

D'autre part, la structure du groupe G/g trouvée à la question précédente montre que G/g possède un 3e sous-groupe à deux éléments constitué des classes g et ag ; ag n'étant ni un élément de g_1/g ni un élément de g_2/g, c'est-à-dire a étant un élément de G n'appartenant ni à g_1 ni à g_2. L'ensemble $g_3 = g \cup ag$ constitue alors un 3e sous-groupe invariant, puisqu'il est image réciproque par l'homomorphisme :

$$G \longrightarrow G/g$$

du sous-groupe invariant $\{e, a\}$. Nous pouvons donc énoncer :

Tout groupe, qui possède deux sous-groupes distincts d'ordre moitié du sien, en possède un troisième distinct des deux précédents.

Exercice 25.

1) Observons d'abord que A^n est l'ensemble des produits de n éléments de A distincts ou non.

Ceci dit, il est évident que toute partie stable contenant A doit contenir A^n pour toute valeur de A, c'est-à-dire $\tilde{A}$.

Il nous reste à vérifier que $\tilde{A}$ est une partie stable. Soit alors :

$$a \in A^n \subset \tilde{A} \qquad a' \in A^{n'} \subset \tilde{A}$$

aa' est le produit de $n + n'$ éléments de A ; il appartient donc à $A^{n+n'}$.

On peut donc conclure que :

$$a \in \tilde{A},\ a' \in \tilde{A} \ \Rightarrow\ aa' \in \tilde{A}.$$

C'est-à-dire que $\tilde{A}$ est stable.

2) Pour qu'une partie stable contenant A soit un sous-groupe il faut d'abord qu'elle contienne tous les inverses des éléments de A, c'est-à-dire tous les éléments de A^{-1}. Elle doit donc contenir :

$$B = A \cup A^{-1}.$$

Mais alors d'après 1) elle doit contenir $\tilde{B}$.

Reste à vérifier que $\tilde{B}$ est un groupe. Nous savons déjà qu'il est une partie stable. Ensuite si $x \in A \subset B$, $x^{-1} \in A^{-1} \subset B$, donc :

$$e = xx^{-1} \in B^2.$$

Enfin, tout élément de $\tilde{B}$ étant un produit d'éléments de $A \cup A^{-1}$ admet dans $\tilde{B}$ un inverse qui est le produit des inverses pris dans l'ordre opposé.

Le plus petit sous-groupe contenant A *est donc bien* $\widetilde{A \cup A^{-1}}$.

Exercice 26.

1) Le plus petit sous-groupe contenant $A \cup B$ contient tout produit en nombre fini quelconque d'éléments appartenant à A et à B. Or, l'associativité de l'opération de groupe permet de remplacer plusieurs éléments consécutifs appartenant à A par leur produit qui appartient aussi à A et de même pour plusieurs éléments consécutifs appartenant à B. Tout élément de g apparaît alors comme le produit d'une suite d'éléments appartenant alternativement à A et à B.

On peut, par ailleurs, vérifier que l'ensemble de ces produits constitue bien un sous-groupe. [Le produit de deux tels produits appartient à leur famille et l'inverse d'un tel produit étant le produit des inverses de ses facteurs, appartient encore à leur famille].

2) Dire que A et B sont permutables, c'est dire que :

$$\forall a_i \in A \qquad \forall b_i \in B \qquad \exists a'_i \in A \qquad \exists b'_i \in B \qquad a_ib_i = b'_ia'_i.$$

S'il en est ainsi, soient deux éléments de AB :

$$a_ib_i \quad \text{et} \quad a_kb_k$$

$$(a_ib_i)(a_kb_k) = a_i(b_ia_k)b_k = a_i(a'_kb'_i)b_k = (a_ia'_k)(b'_ib_k) = a_lb_l.$$

D'autre part, l'inverse d'un élément de AB appartient à AB car :

$$(a_ib_i)^{-1} = (b'_ia'_i)^{-1} = a'^{-1}_i b'^{-1}_i.$$

Donc AB est un sous-groupe. Il est évident que c'est le plus petit, toute partie stable contenant A et B devant contenir AB.

Réciproquement, si AB est un sous-groupe, c'est que :

$$\forall a_i \quad \forall b_i \quad \forall a_j \quad \forall b_j \qquad \exists a_k \quad \exists b_k \qquad a_ib_ia_jb_j = a_kb_k.$$

Multiplions cette égalité, à gauche par a_i^{-1} et à droite par b_j^{-1}. Il vient :

$$b_ia_j = (a_i^{-1}a_k)(b_kb_j^{-1}) = a_lb_l.$$

Donc :

$$\forall a_j \quad \forall b_j \qquad \exists a_l \quad \exists b_l \qquad b_ia_j = a_lb_l.$$

On peut conclure :

$$BA \subset AB.$$

Mais quand a_i et a_j décrivent tout A, b_i et b_j tout B, a_ib_i et a_jb_j décrivent tout AB ; leur produit a_kb_k, produit de deux éléments du sous-groupe AB, décrit aussi tout le sous-groupe. Donc a_k décrit tout A, a_i^{-1} aussi, donc a_l aussi ; il en est de même pour b_l ; et a_lb_l décrit tout AB. On peut donc préciser :

$$BA = AB$$

donc A et B sont permutables.

Si un des groupes A et B est invariant, soit par exemple A, c'est, par définition, que :

$$\forall x \in G \qquad xA = Ax$$

ce qui comporte naturellement :

$$\forall b \in B \qquad bA = Ab.$$

Il en résulte donc que A et B sont permutables (et même de façon un peu particulière puisque dans l'égalité $a_ib_i = b'_ia'_i$ de tout à l'heure on a cette fois $b_i = b'_i$).

Un sous-groupe invariant permute avec un sous-groupe quelconque. En conséquence, le plus petit sous-groupe contenant deux sous-groupes dont l'un est invariant est le produit de ces sous-groupes.

3) Etant donnés deux sous-groupes d'un groupe G on pourra toujours définir leur borne supérieure (la relation d'ordre étant l'inclusion) comme elle l'a été au 1. Quant à leur borne inférieure, elle sera constituée par l'intersection puisque l'intersection de deux sous-groupes est un sous-groupe et que tout sous-groupe contenu dans A et B doit être contenu dans $A \cap B$.

Si maintenant on considère la famille des sous-groupes invariants la 2e question montre que :

$$g_1 \vee g_2 = g_1 g_2.$$

Pour conclure que :

$$g_1 \wedge g_2 = g_1 \cap g_2.$$

il reste seulement à vérifier que l'intersection de deux sous-groupes invariants est un sous-groupe invariant.

Or si $\gamma \in g_1 \cap g_2$

$\forall x \in G$ $\quad x\gamma x^{-1} \in g_1$ puisque g_1 est invariant
$\quad\quad\quad\quad x\gamma x^{-1} \in g_2$ puisque g_2 est invariant

donc : $x\gamma x^{-1} \in g_1 \cap g_2$ et $g_1 \cap g_2$ est invariant.

4) Montrons que A et $B \cap C$ sont permutables. Puisque A et B le sont c'est que :

$$\forall a_i \in A, \quad \forall b_i \in B \qquad \exists a'_i \in A \quad \exists b'_i \in B \qquad a_ib_i = b'_ia'_i \qquad (1)$$

Supposons que b_i appartienne aussi à C (donc à $B \cap C$) comme $a_i \in A \subset C$, $a_ib_i \in C$. Mais $a'_i \in C$; la propriété fondamentale de résolution des équations dans les groupes montre que b_i appartient à C, donc à $B \cap C$. L'égalité (1) exprime alors la permutabilité de A et de $B \cap C$.

Montrons maintenant : $\quad A(B \cap C) = C \cap AB.$

1) $\quad x \in A(B \cap C) \Rightarrow x = ab \left\{ \begin{array}{l} a \in A \subset C \\ b \in B \\ b \in C \end{array} \right\} \Rightarrow ab \in C \Rightarrow x \in AB \cap C$

2) $\quad y \in AB \cap C \Rightarrow y \in C,\ y = ab \left\{ \begin{array}{l} a \in A \subset C \\ b \in B \end{array} \right.$

Or : $\quad ab \in C \quad a \in C \Rightarrow \quad b \in C \Rightarrow b \in B \cap C \Rightarrow \quad y \in A(B \cap C)$

donc : $\quad y \in AB \cap C \Rightarrow y \in A(B \cap C).$

1) et 2) démontrent donc l'égalité. Or en tenant compte de ce que nous avons dit au 3, elle s'écrit :

$$A \vee (B \wedge C) = C \wedge (A \vee B).$$

Dans le cas général, comparons $A \vee (B \wedge C)$ et $(A \vee B) \wedge C$.

Nous avons d'après les hypothèses :

$$A \prec A \vee B \qquad A \prec C$$
$$B \wedge C \prec C \qquad B \wedge C \prec B \prec A \vee B.$$

Nous avons donc à comparer $\sup \{ a, b \}$ et $\inf \{ c, d \}$, les deux éléments du couple a, b étant antérieurs aux deux éléments du couple c, d. La définition même des bornes inférieures et supérieures prouve que :

$\sup \{ a, b \} \prec c$, $\sup \{ a, b \} \prec d$ donc $\sup \{ a, b \} \prec \inf \{ c, d \}$.

L'implication demandée est donc établie.

5) Remarquons d'abord que $A \cap B$ est un sous-groupe invariant de B. En effet si $a \in A \cap B$:

$\forall x \in B$ $\quad xax^{-1} \in B$ puisque B est un sous-groupe
$\quad\quad\quad\quad xax^{-1} \in A$ puisque A est invariant

donc $xax^{-1} \in A \cap B$ et ce sous-groupe est invariant.

Ceci dit, considérons les groupes quotients $B/A \cap B$ et AB/A.

Le premier est l'ensemble des classes :

$$(A \cap B)b \qquad \text{où } b \text{ décrit B.}$$

Le deuxième est l'ensemble des classes :

$$Aab \qquad \text{où } ab \text{ décrit AB.}$$

Mais $Aa = A$ et toutes les classes Aab où b est fixe et a décrit A sont confondues. L'ensemble AB/A est donc l'ensemble des classes : Ab où b décrit B.

Ceci dit, considérons la bijection :

$$\dot{b} = (A \cap B)b \longrightarrow \overline{b} = Ab.$$

Puisque $B \longrightarrow B/A \cap B$ et $AB \longrightarrow AB/A$ sont des homomorphismes :

$$\dot{b}\dot{b'} = \widehat{\dot{b}\dot{b'}} \qquad \overline{b}\,\overline{b'} = \overline{bb'}$$

et il en résulte que la bijection précédente est un isomorphisme.

Exercice 27.

Soit $a \in G$. Il engendre un groupe cyclique U_1 d'ordre λ_1 ; ce sous-groupe est invariant puisque G est abélien. Considérons alors le groupe quotient G/U_1. S'il est cyclique la propriété est démontrée.

S'il ne l'est pas, soit $a_2 \in G$, $a_2 \notin U_1$ et considérons l'ensemble :

$$U_2 = \bigcup_{i \in Z} a_2^i U_1$$

On vérifiera aisément que G étant abélien, U_2 constitue un groupe dont U_1 est un sous-groupe invariant. U_2/U_1 est engendré par l'élément a_2U_1. U_2 étant fini, le groupe U_2/U_1 est fini, donc cyclique puisque monogène ; c'est dire qu'il existe un entier λ_2 tel que :

$$a_2^{\lambda_2} U_1 = U_1$$

c'est-à-dire tel que :

$$a_2^{\lambda_2} \in U_1.$$

On aura alors :

$$U_2 = \bigcup \{ a_2^i U_1 \ ; \ 0 \leqslant i \leqslant \lambda_2 - 1 \}$$

et on voit que U_2 est d'ordre $\lambda_1\lambda_2$. Si maintenant G/U_2 est cyclique la propriété est démontrée.

Sinon, soit $a_3 \in G \quad a_3 \notin U_2$ et considérons :

$$U_3 = \bigcup_{i \in Z} a_3^i U_2 = \bigcup \{ a_3^i U_3 ; \ 0 \leqslant i \leqslant \lambda_3 - 1 \}$$

λ_3 étant le plus petit entier tel que $a_3^{\lambda_3} \in U_2$. On montrera comme précédemment que U_3 est un groupe d'ordre $\lambda_1\lambda_2\lambda_3$ et que U_3/U_2 est cyclique d'ordre λ_3... et ainsi de suite...

L'ordre de chaque groupe U_k étant un multiple de l'ordre du groupe U_{k-1} précédemment considéré et l'ordre de G étant fini, le processus s'arrêtera au bout d'un nombre fini d'opérations.

Exemple : G : groupe multiplicatif des entiers $\neq 0$ modulo 19.

Prenons $a_1 = 7$,

on a : $7^3 = 1$ soit $U_1 = \{ 1, 7, 7^2 = 11 \}$.

Prenons $a_2 = 5$,

$5^3 = 11$ donc $5^3 U_1 = \{ 11, 7, 1 \} = U_1$

$U_2 = \{ 5^i U_1 \}$ avec $i = 0, 1, 2$.

U_2 a 9 éléments et $2U_2$ contient les 9 autres éléments de G ; 2^2U_2 serait égal à U_2 ($2^2 = 4 \in 5^2U_1$, donc $2^2 \in U_2$).

On a donc :

G/U_2 cyclique d'ordre	2	(isomorphe à Z_2)
U_2/U_1	3	..... Z_3
U_1	3	..... Z_3

2) Observons d'abord que quand l'ordre d'un groupe est premier il est simple. Mais inversement si l'ordre d'un groupe cyclique n'est pas premier il admet des sous-groupes. En effet, soit $n = pq$ l'ordre d'un groupe cyclique et soit x son générateur.

$$x^{pq} = e$$

peut s'écrire $(x^p)^q = e$, ce qui montre que x^p engendre un sous-groupe cyclique d'ordre q (et x^q un sous-groupe d'ordre p) (*).

Si donc λ_{i+1} n'est pas premier, U_{i+1}/U_i ne sera pas simple et admettra un sous-groupe engendré par une puissance de l'élément générateur de U_{i+1}/U_i, c'est-à-dire par :

$$a_i^k \ U_i.$$

Au lieu de construire U_{i+1} à l'aide de l'élément a_i comme ci-dessus nous construirons :

$$V = \bigcup \{ a_i^{k\mu} U_i ; \ 0 \leqslant k\mu \leqslant \lambda_i - 1 \}$$

Nous aurons :

$$U_i \subset V \subset U_{i+1}$$

V/U_i sera un groupe cyclique d'ordre $\frac{\lambda_i}{k}$ et U_{i+1}/V sera un groupe cyclique d'ordre k (élément générateur a_iV avec $(a_iV)^k = V$).

Si l'un ou l'autre des deux groupes U_{i+1}/V et V/U_i n'est pas simple

(*) Observons d'ailleurs que les sous-groupes de cette nature sont les seuls que puissent posséder un groupe cyclique. Car si un tel groupe possédait un sous-groupe qui ne soit pas monogène, c'est-à-dire admette deux générateurs x^p et x^q, il contiendrait $x^{\lambda p + \mu q}$ (λ et μ étant des entiers quelconques) et donc x^D, D étant le P.G.C.D. de p et q ; on voit alors qu'il admettrait x^D comme générateur unique.

nous pourrons recommencer l'opération, et ainsi de suite jusqu'à ce que tous les groupes soient simples.

Le nombre de groupes de la chaîne sera donc égal au nombre de facteurs premiers de la décomposition de l'ordre de G et leurs ordres seront, à l'ordre près, les facteurs de cette décomposition. Dans notre exemple de tout à l'heure si nous étions partis de $a_1 = 8$ nous aurions engendré $U_1 = \{ 1, 8, 7, 18, 11, 12 \}$ et $G/U_1 = \{ 3^i U_1 \}$ avec $i = 0, 1, 2$, mais U_1 n'est pas simple et admet, par exemple, pour sous-groupe $\{ 1, 18 \} = V$, nous aurons $U_1/V = \{ 7^i V \}$ avec $i = 0, 1, 2$ et nous aurons :

$V \subset U_1 \subset G$	G/U_1 cyclique d'ordre	3
	U_1/V	3
	V	2

Quels que soient les choix faits, nous aurons finalement une suite de trois groupes cycliques ayant respectivement pour ordre les facteurs premiers de 18.

Exercice 28.

On vérifie immédiatement que $g_1 \times g_2$ est un sous-groupe de $G_1 \times G_2$:

$$\forall (a_1, a_2) \in g_1 \times g_2, \quad (b_1, b_2) \in g_1 \times g_2$$
$$(a_1, a_2) \times (b_1, b_2) = (a_1 b_1, a_2 b_2) \in g_1 \times g_2$$

$$\forall (a_1, a_2) \in g_1 \times g_2 \qquad (a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1}) \in g_1 \times g_2$$

et que ce sous-groupe est invariant :

$$\forall (x_1, x_2) \in G_1 \times G_2, \ \forall (a_1, a_2) \in g_1 \times g_2$$
$$(x_1, x_2).(a_1, a_2).(x_1^{-1}, x_2^{-1}) = (x_1 a_1 x_1^{-1}, x_2 a_2 x_2^{-1}) = (a'_1, a'_2) \in g_1 \times g_2.$$

Ceci dit,

G_1/g_1 est l'ensemble des classes $\{ x_1 g_1 ; \ x_1 \in G_1 \}$

G_2/g_2 ..... $\{ x_2 g_2 ; \ x_2 \in G_2 \}$

et un élément de $G_1/g_1 \times G_2/g_2$ sera $(x_1 g_1, x_2 g_2)$, l'ensemble étant décrit quand (x_1, x_2) décrit $G_1 \times G_2$.

D'autre part, la classe modulo $g_1 \times g_2$ de l'élément $(x_1, x_2) \in G_1 \times G_2$, classe que nous noterons $\overline{(x_1, x_2)}$, est formée de tous les éléments :

$$(x_1 a_1, x_2 a_2)$$

où a_1 décrit g_1 et a_2 décrit g_2 ; donc elle est l'ensemble :

$$\{ (y_1, y_2) ; \ y_1 \in x_1 g_1, \ y_2 \in x_2 g_2 \}$$

et $G_1 \times G_2/g_1 \times g_2$ sera décrit par l'élément ci-dessus quand (x_1, x_2) décrit $G_1 \times G_2$.

Il est alors évident qu'il existe une bijection :

$$G_1/g_1 \times G_2/g_2 \longrightarrow G_1 \times G_2/g_1 \times g_2,$$

$$(x_1 g_1, x_2 g_2) \longrightarrow \overline{(x_1, x_2)} = \{ (y_1, y_2) ; \ y_1 \in x_1 g_1, \ y_2 \in x_2 g_2 \},$$

et il est évident aussi que cette bijection est un isomorphisme puisque :

$$(x_1 g_1, x_2 g_2)\ (x'_1 g_1, x'_2 g_2) = (x_1 x'_1 g_1, x_2 x'_2 g_2),$$

et d'autre part le composé de deux classes de $G_1 \times G_2$ (modulo $g_1 \times g_2$) est la classe du composé soit :

$$\overline{(x_1 x'_1, x_2 x'_2)} = \{ (y_1, y_2) ; \ y_1 \in x_1 x'_1 g_1, \ y_2 \in x_2 x'_2 g_2 \}.$$

On peut donc conclure :

$$G_1/g_1 \times G_2/g_2 \approx G_1 \times G_2/g_1 \times g_2.$$

Exemple : $G_1 = G_2 = \mathbf{R} \quad g_1 = m\mathbf{Z} \ g_2 = n\mathbf{Z} \quad m, n \in \mathbf{R}.$

Un élément de $\mathbf{R}/m\mathbf{Z} \times \mathbf{R}/n\mathbf{Z}$ est le couple formé par la famille des droites d'abscisses $hm + \lambda$ et la famille des droites d'ordonnées $kn + \mu$ (λ et μ fixes, h et k décrivant $\mathbf{Z}$).

Un élément de $\mathbf{R}^2/m\mathbf{Z} \times n\mathbf{Z}$ est l'ensemble des points dont les coordonnées sont de la forme $hm + \lambda$, $kn + \mu$, c'est-à-dire les points d'un réseau.

Exercice 29.

1) Si $G \approx (G/H) \times H$ c'est que G/H est isomorphe à un sous-groupe invariant g' de G et que G/g' est isomorphe à H. Il y a donc un homomorphisme f de G sur H où tout élément x de H est l'image de sa classe modulo g' :

$$\overset{-1}{f}(x) = xg',$$

or $xg' \ni x$ donc $\overset{-1}{f}(x) \ni x$ et $f(x) = x$.

2) Réciproquement, s'il existe un homomorphisme de G sur H, étant donné qu'il en existe aussi un de G sur G/H, nous pouvons faire le schéma suivant :

$$\begin{array}{ccccc} G/H & \longleftarrow & G & \xrightarrow{\ f\ } & H \\ \dot{a} & \longleftarrow & a & \longrightarrow & \alpha \\ & & \downarrow \varphi & & \\ & & G/H \times H & & \\ & & (\dot{a}, \alpha) & & \end{array}$$

C'est-à-dire qu'à un élément de G nous faisons correspondre le couple formé de sa classe (modulo H) et de son image dans l'homomorphisme f, ce qui revient à définir une application φ de G sur le produit cartésien de G/H et de H.

On voit tout de suite que φ est un homomorphisme. Soient, en effet, deux éléments a et b de G :

$$\varphi(ab) = (\dot{\widehat{ab}}, f(ab)),$$
$$\varphi(a) \times \varphi(b) = (\dot{a}\dot{b}, \alpha\beta).$$

Or l'application canonique étant un homomorphisme $\dot{\widehat{ab}} = \dot{a}\dot{b}$, et, f étant un homomorphisme $f(ab) = f(a)\,f(b) = \alpha\beta$.

Pour montrer l'isomorphisme $G \approx (G/H) \times H$ il reste donc seulement à montrer que φ est une bijection, ce qui (φ étant évidemment surjective) revient à montrer qu'elle est injective, c'est-à-dire que deux éléments différents de G n'ont pas la même image dans $(G/H) \times H$, or deux éléments qui auraient même image (a, α) appartiendraient nécessairement à la classe de a ; ce seraient donc ax et ax', $x \in H$, $x' \in H$. Pour que $f(ax) = f(ax')$ il faudrait que $f(a)f(x) = f(a)f(x')$, ce qui est impossible si $x \neq x'$ puisque $f(x) = x$ pour tout x.

Exercice 30.

Considérons la classe U dans G (modulo H) qui est l'élément générateur du groupe monogène G/H. Cette classe est de la forme xH, $x \in$ G, $x \notin$ H.

G/H étant monogène est formé des classes :

$$e = \text{H, U, U}^2 \ldots \text{U}^\lambda \ldots,$$

c'est-à-dire de H et des classes dans G (modulo H) de :

$$x, x^2 \ldots x^\lambda \ldots$$

Si $\forall\lambda \quad x^\lambda \notin$ H,

U engendre le groupe monogène infini :

$$\{ \text{U}^\lambda \,;\, \lambda \in \mathbf{Z} \} \qquad \text{avec } \text{U}^\lambda = x^\lambda \text{H}$$

et G/H est isomorphe au sous-groupe G' de G formé des puissances de x, et tout élément de G, appartenant à une seule classe (modulo H), peut s'écrire de manière unique sous la forme :

$$x^\lambda a,$$

λ décrivant $\mathbf{Z}$ et a décrivant H, c'est-à-dire :

$$x^\lambda \in \text{G}' \quad a \in \text{H}.$$

Nous sommes maintenant en mesure d'affirmer que G est le produit direct de G' et de H [donc est isomorphe à $(G/H) \times H$] puisque tout élément de G se factorise de manière unique en un élément de G' et un élément de H. (Le groupe étant abélien, la condition de permutabilité est automatiquement satisfaite).

Remarque : Notons le rôle joué par l'hypothèse « G/H infini ». Si G/H avait été fini, donc cyclique, c'est qu'il aurait existé un entier λ_0 tel que $x^{\lambda_0} \in$ H. Tous les éléments $x^{\lambda + k\lambda_0}$ appartiennent à la même classe que x et un même élément de G pourra se factoriser d'une infinité de façons en un élément de H et un élément de G' puisqu'il pourra s'écrire :

$$x^\lambda a = x^{\lambda + k\lambda_0} \cdot a x^{-k\lambda_0} \qquad \begin{array}{l} x^{\lambda + k\lambda_0} \in \text{G}' \\ a x^{-k\lambda_0} \in \text{H}. \end{array}$$

Exercice 31.

(1) Notons que $|a + b| = (a + b)^+ - (a + b)^-$
et que $|a| + |b| = a^+ + b^+ - a^- - b^-$.

Or, on peut écrire d'après la définition même du symbole a^+ :

$$\left.\begin{array}{l} a^+ \succ 0 \\ b^+ \succ 0 \end{array}\right\} \Rightarrow a^+ + b^+ \succ 0 \qquad \left.\begin{array}{l} a^+ \succ a \\ b^+ \succ b \end{array}\right\} \Rightarrow a^+ + b^+ \succ a + b \qquad \left.\begin{array}{l} \\ \\ \end{array}\right\} \Rightarrow a^+ + b^+ \succ (a + b)^+ \quad (1)$$

et de même :

$$a^- + b^- \prec (a + b)^-$$

ou :

$$-a^- - b^- \succ -(a + b)^- \qquad (2),$$

et en ajoutant (1) et (2) membres à membres nous trouvons la relation à démontrer.

(2) $\qquad |a - b| = (a - b)^+ - (a - b)^-$

Or, on sait que si on ajoute b à deux nombres, leur inf et leur sup augmentent de b. Donc :

$$(a - b)^+ = a \vee b - b$$
$$(a - b)^- = a \wedge b - b$$

D'où $\qquad |a - b| = a \vee b - a \wedge b.$

Exercice 32 (sur les groupes réticulés).

1) $\left.\begin{matrix} a \vee b \succ a \Rightarrow -(a \vee b) \prec -a \\ a \vee b \succ b \Rightarrow -(a \vee b) \prec -b \end{matrix}\right\} \Rightarrow -(a \vee b) \prec (-a) \wedge (-b) \qquad (1)$

On démontrerait de la même façon par échange des signes $\prec$ et $\succ$, $\vee$ et $\wedge$ que :

$$-(a \wedge b) \succ (-a) \vee (-b).$$

Appliquons cette formule aux nombres $(-a)$ et $(-b)$. Il vient :

$$-[(-a) \wedge (-b)] \succ a \vee b$$

ou $$(-a) \wedge (-b) \prec -(a \vee b),$$

formule qui, rapprochée de (1), établit la propriété demandée.

2) *a*) Si la première égalité est démontrée pour la relation notée $\prec$, il suffit de considérer la relation inverse notée $\succ$, les inf relativement à la relation $\prec$ deviennent les sup relativement à la relation $\succ$ et réciproquement et la deuxième égalité sera également démontrée.

b) Dans tout treillis on peut écrire :

$$\left.\begin{matrix} c \prec a \vee c \\ c \prec b \vee c \end{matrix}\right\} \Rightarrow c \prec (a \vee c) \wedge (b \vee c)$$

$$\left.\begin{matrix} a \wedge b \prec a \prec a \vee c \\ a \wedge b \prec b \prec b \vee c \end{matrix}\right\} \Rightarrow a \wedge b \prec (a \vee c) \wedge (b \vee c),$$

c et $a \wedge b$ étant antérieurs à un même nombre, leur sup l'est aussi et l'inégalité est démontrée.

c) α) Supposons l'inégalité démontrée dans le cas où $a \wedge b = 0$ et soient maintenant a et b tels que $a \wedge b = m$. Nous aurons :

$$(a - m) \wedge (b - m) = 0$$

et pourrons écrire :

$$[(a - m) \wedge (b - m)] \vee c \succ [(a - m) \vee c] \wedge [(b - m) \vee c].$$

Augmentons alors de m chacun des nombres $a - m$, $b - m$ et c ; les inf et sup figurant dans l'inégalité augmentent de m et l'inégalité reste vraie ; ce qui donne :

$$[a \wedge b] \vee (c + m) \succ [a \vee (c + m)] \wedge [b \vee (c + m)]$$

Il est clair que m étant quelconque, $c + m$ l'est aussi et l'inégalité sera démontrée en général.

β) Remarquons en outre que :

$$\left.\begin{matrix} a \vee c \succ a \\ a \vee c \succ a \succ 0 \\ a \vee c \succ c \end{matrix}\right\} \Rightarrow a \vee c \succ 0 \vee c = c^+ \Rightarrow a \vee c \succ a \vee c^+$$

et

$$\left.\begin{matrix} a \vee c^+ \succ a \\ a \vee c^+ \succ c \end{matrix}\right\} \Rightarrow a \vee c^+ \succ a \vee c,$$

soit

$$a \vee c^+ = a \vee c.$$

Les remarques α) et β) montrent qu'il suffit de démontrer l'inégalité

$0 \vee c \succ (a \vee c^+) \wedge (b \vee c^+)$ avec $a \wedge b = 0$,

or $0 \vee c = c^+$. Il suffit donc de montrer que :

$$c^+ \succ (a \vee c^+) \wedge (b \vee c^+)$$

ou l'inégalité équivalente :

$$0 \succ [(a - c^+) \vee 0] \wedge [(b - c^+) \vee 0].$$

Mais puisque $c^+ \succ 0$ $\quad a - c^+ \prec a$ et $(a - c^+) \vee 0 \prec a$.

De même $(b - c^+) \vee 0 \prec b$ et leur sup est antérieur à $a \wedge b = 0$, ce qui démontre l'inégalité.

3) Nous démontrerons cette égalité par récurrence. Pour $n = 2$ on peut écrire :

$$2(a \wedge 0) = a \wedge 0 + a \wedge 0.$$

Or, pour ajouter $a \wedge 0$ à un sup, nous pouvons l'ajouter aux deux nombres. Il vient :

$2(a \wedge 0) = [a + a \wedge 0] \wedge (a \wedge 0) = (2a \wedge a) \wedge (a \wedge 0) = 2a \wedge a \wedge 0.$

Si maintenant l'égalité est démontrée pour le rang $n - 1$:

$$(n - 1)(a \wedge 0) = (n - 1)a \wedge (n - 2)a \ldots\ldots \wedge 2a \wedge a \wedge 0.$$

Ajoutons $a \wedge 0$ aux deux membres, ce que nous ferons dans le deuxième membre en ajoutant $a \wedge 0$ à chacun des nombres ; en tenant compte de ce que

$$pa + a \wedge 0 = (p + 1)\, a \wedge pa,$$

on trouve :

$$n(a \wedge 0) = na \wedge (n - 1)a \ldots\ldots\ldots \wedge 2a \wedge a \wedge 0.$$

Supposons alors que $na \succ 0$. L'opération indiquée dans le deuxième membre est, de par sa définition même, associative et commutative. Donc $na \wedge 0$ étant égal à 0 puisque $na \succ 0$, on peut supprimer na de la suite du deuxième membre. Mais alors ce deuxième membre vaut $(n - 1)(a \wedge 0)$ et on peut écrire :

$$n(a \wedge 0) = (n - 1)(a \wedge 0) \Rightarrow a \wedge 0 = 0 \Rightarrow a \succ 0.$$

4) $a^+ \wedge -(a^-) = (a \vee 0) \wedge -(a \wedge 0)$.

Or, le 1) nous permet d'écrire : $-(a \wedge 0) = (-a) \vee 0$.

D'où $a^+ \wedge -(a^-) = (a \vee 0) \wedge (-a \vee 0) = (a \wedge -a) \vee 0$,

en appliquant la propriété de distributivité démontrée au 2).

Mais $a \wedge -a \prec a$

$a \wedge -a \prec -a$,

ajoutons membres à membres ; il vient :

$$2(a \wedge -a) \prec 0,$$

ce qui implique :

$a \wedge -a \prec 0$ en vertu du 3). (On démontrerait $na \prec 0 \Rightarrow a \prec 0$ de la même façon que $na \succ 0 \Rightarrow a \succ 0$).

Donc $(a \wedge -a) \vee 0 = 0$,

et par conséquent :

$$a^+ \wedge -(a^-) = 0.$$

Exercice 33.

Additionnons les deux égalités membres à membres. Il vient :

$$a \vee x + a \wedge x = a \vee y + a \wedge y,$$

et en tenant compte de la propriété démontrée page 51 :

$$a + x = a + y,$$

soit $$x = y.$$

Exercice 34.

Soit G le groupe des opérateurs, E l'ensemble donné et considérons l'application :

$$\mathrm{E} \longrightarrow \mathrm{E}$$

$$x \xrightarrow{(\alpha)} \alpha x \qquad \alpha \in \mathrm{G}.$$

Montrons que c'est une bijection :

1) Elle est surjective. En effet, tout $y \in \mathrm{E}$ a une image y' dans l'application (α^{-1}). Faisons alors subir à (y') l'application (α). Son image $\alpha y'$ sera, d'après l'hypothèse :

$$\alpha y' = \alpha(\alpha^{-1}y) = (\alpha\alpha^{-1})y = \varepsilon y = y,$$

donc $\quad \forall y \in E, \quad \exists y' \in E \quad y = \alpha y'.$

2) Elle est injective. Supposons en effet que deux éléments x et y aient la même image : $\alpha x = \alpha y$. Dans l'application (α^{-1}) cette image a une image unique. Or,

$$\alpha^{-1}(\alpha x) = x \qquad \alpha^{-1}(\alpha y) = y.$$

Donc $\quad \alpha x = \alpha y \Rightarrow x = y.$

On a donc défini une application du groupe G dans le groupe S_E des bijections sur E.

$$G \longrightarrow S_E$$
$$\alpha \longrightarrow (\alpha).$$

Il est clair que cette application est un homomorphisme puisque :

$$(\alpha)\circ(\beta) = (\alpha\beta).$$

L'image de G est donc un sous-groupe de S_E.

Remarque : Nous disons bien homomorphisme et non isomorphisme car plusieurs opérateurs différents peuvent donner la même bijection. Dans ce cas, le sous-groupe de S_E est isomorphe à un groupe quotient G/g, g étant le sous-groupe invariant de G formé des éléments α_0 de G tels que $\alpha_0 x = x, \quad \forall x \in E$.

Exemple : Soit E une droite d'un plan et soit G le groupe des isométries de ce plan qui laissent E invariante : translation T parallèle à E, symétrie Σ par rapport à E, symétries S par rapport à chacun des points de E, symétries S′ par rapport aux perpendiculaires à E. Le groupe g est constitué de la transformation identique et de la symétrie Σ ; une classe de G (modulo g) contient les deux transformations T et $T\circ\Sigma = \Sigma\circ T$ (ou S et $S\circ\Sigma = \Sigma\circ S$ qui est une S′ ou encore S′ et $S'\circ\Sigma = \Sigma\circ S'$ qui est une S) qui donnent la même bijection de E sur elle-même.

Exercice 35.

1) Notons $\times$ la loi cherchée.

Observons d'abord que, cette loi donnant à Z une structure d'anneau, nous devrons avoir :

$$0 \times x = x \times 0 \qquad \forall x \in Z.$$

Ensuite, pour que cette opération induise sur N la multiplication il faut que :

$$(c, 0) \times (c', 0) = (c', 0) \times (c, 0) = (cc', 0).$$

Soit alors le nombre $(0, c)$ opposé du nombre $(c, 0)$; la distributivité de l'opération entraîne :

$$[(0, c) + (c, 0)] \times (c', 0) = 0 \text{ et } (c', 0) \times [(0, c) + (c, 0)] = 0,$$

d'où

$$(0, c) \times (c', 0) = \text{opposé de } (c, 0) \times (c', 0) = (0, cc'),$$

et de même :

$$(c', 0) \times (0, c) = \text{opposé de } (c', 0) \times (c, 0) = (0, cc').$$

Enfin, en raisonnant de la même manière, on trouve que $(0, c)\times(0, c')$ et $(0, c') \times (0,c)$ doivent être tous deux égaux à l'opposé du produit calculé ci-dessus, c'est-à-dire à $(cc', 0)$.

Propriétés : Nous avons donc établi :

1) que l'opération est *commutative* ;

2) si nous remarquons que dans $(c, 0)$ ou dans $(0, c)$, c représente ce que l'on appelle en algèbre élémentaire la valeur absolue du nombre relatif (c'est aussi la valeur absolue au sens donné dans le chapitre des groupes réticulés comme il est aisé de le vérifier), nous avons établi que

la *valeur absolue du produit* est le produit des valeurs absolues ainsi que la « *règle des signes* ». Seul 0 ayant 0 pour valeur absolue, pour que 0 ait un diviseur il faudrait que sa valeur absolue divise 0. Or, le produit de deux entiers naturels n'est jamais nul. *Dans Z il n'y a pas de diviseurs de* 0.

L'associativité de l'opération résulte de l'associativité du produit des valeurs absolues et de la règle des signes, enfin, la *distributivité* par rapport à l'addition se vérifie aisément. Z étant alors muni d'une opération de groupe (l'addition) et d'une deuxième opération associative et distributive par rapport à la première est *un anneau.*

En nous reportant à l'ordre sur Z (cf. page 57), notons que (les lettres désignant maintenant des éléments de Z) :

$$c > 0, a < b \Rightarrow a - b < 0 \Rightarrow c(a - b) < 0 \Rightarrow ca < cb.$$
$$c < 0, a < b \Rightarrow a - b < 0 \Rightarrow c(a - b) > 0 \Rightarrow ca > cb.$$

Remarque : Nous avons établi la définition de la multiplication en utilisant la représentation canonique d'un élément de Z. Un élément de cette forme caractérisant sa classe, la méthode est légitime et elle est la plus rapide. Mais nous aurions pu aussi définir une multiplication sur les classes de N^2/R. C'est la méthode que nous serons contraints d'employer pour définir l'addition dans Q.

2) L'absence de diviseurs de 0 dans Z permet d'écrire que si

$$c \neq 0, ca = cb \Rightarrow c(a - b) = 0 \Rightarrow a - b = 0 \Rightarrow a = b,$$

$Z - \{0\}$ que nous appellerons Z^* sur lequel est définie une multiplication associative, commutative et simplifiable est un demi-groupe commutatif. Si on le plonge dans le plus petit groupe commutatif qui le contient, que nous appellerons Q^* et si on ajoute 0 à cet ensemble, on obtient Q.

On sait d'après le théorème général que Q^* et son opération de groupe sont déterminés d'une manière unique à un isomorphisme près.

$$Q^* = \{\dot{(a, b)} ; \dot{(a, b)} \in Z^{*2}/R\} = Z^{*2}/R$$
$$\dot{(a, b)} \times \dot{(a', b')} = \dot{(aa', bb')}$$

(R étant la relation d'équivalence indiquée dans le cours).

Reste maintenant à étendre la multiplication à Q tout entier, c'est-à-dire à déterminer ce que doit être $0x$.

Cette multiplication induit sur Z^* la multiplication définie à la première question. D'autre part, elle doit être distributive par rapport à l'addition que nous allons devoir définir, laquelle devra sur Z induire l'addition de Z. Notre multiplication est donc distributive par rapport à l'addition sur Z ; d'où il résulte que :

$$0n = 0 \qquad \forall n \in Z.$$

Soit alors $0x$, x appartenant à Q^*.

Nous savons qu'il existe $y \in Z^*$ tel que $xy \in Z^*$ [si $x = \dot{(a, b)}$, $y = \dot{(b, 1)}$ car $xy = \dot{(ab, b)} = \dot{(a, 1)}$].

On a alors :

$$(0x)y = 0(xy) = 0,$$

d'après ce qui vient d'être dit. Il est alors impossible que $0x$ appartienne à Q^* car son produit par $y \in Z^* \subset Q^*$ appartiendrait aussi à Q^*. Donc :

$$\forall x \in Q^* \qquad 0x = 0.$$

Or, ceci peut être décrit de façon à ce que 0 ne constitue pas une exception dans Q. Nous pouvons, en effet, poser :

$$\forall b \in Z^* \qquad \dot{(0, b)} = 0.$$

On aura bien $\dot{(0, b)}$ R $\dot{(0, b')}$ puisque $0b' = b0$

et $\dot{(a, c)} \times \dot{(0, b)} = \dot{(0, bc)} = 0,$

ce qui est conforme à la loi générale. Il suffira de poser :

$$0 \times 0 = 0,$$

soit $$\dot{(0, a)} \times \dot{(0, b)} = \dot{(0, ab)}$$

pour que 0 rentre en tous points dans le cas général en ce qui concerne la loi multiplicative sur **Q**.

Observons qu'en revanche les couples $(a, 0)$ n'ont pas été définis et si on cherchait à leur attribuer un sens on aboutirait à des contradictions.

Nous pouvons donc conclure :

$$\mathbf{Q} = \{ \dot{(a, b)} \; ; \dot{(a, b)} \in \frac{\mathbf{Z} \times \mathbf{Z}^*}{\mathrm{R}} \} = (\mathbf{Z} \times \mathbf{Z}^*)/\mathrm{R}$$

ce qui veut dire que a peut prendre toute valeur de **Z** y compris 0, que b au contraire décrit **Z** à l'exclusion de 0, R conservant toujours la même signification.

Soit maintenant à définir une deuxième opération sur **Q** que nous noterons provisoirement $\oplus$ et qui devra satisfaire aux deux propriétés indiquées.

Soient $\dot{(a, b)}$ et $\dot{(c, d)}$ deux éléments de **Q** et $\dot{(a, b)} \oplus \dot{(c, d)}$ leur composé. Multiplions ce nombre par $\dot{(bd, 1)}$ (élément choisi pour que ses produits par $\dot{(a, b)}$ et $\dot{(c, d)}$ appartiennent à **Z**). En vertu de la distributivité désirée, il vient :

$$[\dot{(a, b)} \oplus \dot{(c, d)}]\, \dot{(bd, 1)} = \dot{(a, b)}\, \dot{(bd, 1)} \oplus \dot{(c, d)}, \dot{(bd, 1)}$$

$$= \dot{(abd, b)} \oplus \dot{(cbd, d)} = \dot{(ad, 1)} \oplus \dot{(cb, 1)},$$

et pour que $\oplus$ induise la somme sur **Z** ceci doit être égal à :

$$\dot{(ad + cb, 1)}.$$

Nous avons donc l'égalité :

$$[\dot{(a, b)} \oplus \dot{(c, d)}] \quad \dot{(bd, 1)} = \dot{(ad + cb, 1)}.$$

Multiplions les deux membres par $\dot{(1, bd)}$. Il vient, la multiplication sur **Q** étant associative :

$$\dot{(a, b)} \oplus \dot{(c, d)} = \dot{(ad + cb, bd)}. \qquad (1)$$

Si la loi $\oplus$ existe, c'est celle que définit l'égalité (1). Reste à montrer que la loi ainsi obtenue répond bien à la question, c'est-à-dire :

1) que c'est bien une loi de composition entre éléments de **Q**, c'est-à-dire indépendante du représentant de la classe (mod R) considérée ;

ou encore que :

$(a, b)\mathrm{R}(a', b') \Rightarrow (a, b) \oplus (c, d)\mathrm{R}(a', b') \oplus (c, d)$;

2) qu'elle vérifie bien en général la condition de distributivité (et pas seulement dans le cas particulier qui a servi à trouver la loi), c'est-à-dire que :

$$[\dot{(a, b)} \oplus \dot{(c, d)}]\dot{(e, f)} = \dot{(a, b)}\dot{(e, f)} \oplus \dot{(c, d)}\dot{(e, f)} \; ;$$

3) qu'elle induit bien sur **Z** l'addition :

$$\dot{(a, 1)} \oplus \dot{(b, 1)} = \dot{(a + b, 1)}.$$

Ces trois vérifications sont immédiates. La 3e va nous permettre de remplacer dorénavant le signe $\oplus$ par $+$.

Propriétés : De la règle même et du fait qu'addition et multiplication sur **Z** sont associatives et commutatives, il résulte que l'addition sur **Q** jouit des deux mêmes propriétés.

Pour cette opération **Q** est un groupe car 0 est élément neutre et tout élément $\dot{(a, b)}$ admet pour opposé $\dot{(-a, b)}$. **Q**, groupe par rapport à l'addition et muni d'une loi distributive par rapport à elle et qui est une loi de groupe pour $\mathbf{Q} - \{0\}$, est donc *un corps*.

Ordre sur **Q**. Remarquons enfin que si nous considérons $\mathbf{Q}^+$, tel qu'il a été défini dans le cours (II, 6, 3) par plongement du demi-groupe multiplicatif $\mathbf{N}^*$, nous pourrons le compléter par 0 en prolongeant la multiplication de ce $\mathbf{Q}^+$ à $\mathbf{Q}^+ \cup \{0\}$ (comme nous l'avons fait tout à l'heure pour prolonger celle de $\mathbf{Q}^*$ à **Q**) ; nous aurons alors :

$$\mathbf{Q}^+ \cup \{0\} = \left\{ \dot{(a, b)} \; ; \dot{(a, b)} \in \frac{\mathbf{N} \times \mathbf{N}^*}{\mathrm{R}} \right\}$$

tandis que :

$$\mathbf{Q} = \left\{ \dot{(a, b)} \; ; \dot{(a, b)} \in \frac{\mathbf{Z} \times \mathbf{Z}^*}{\mathrm{R}} \right\}.$$

la relation R considérée pour le premier ensemble étant la restriction à $\mathbf{N} \times \mathbf{N}^*$ de la relation R considérée pour le deuxième. Le premier de ces deux ensembles est donc isomorphe à un sous-ensemble du second, soit $\mathbf{Q}''$.

$$\mathbf{Q}'' = \left\{ \dot{(a, b)} \; ; a \in \mathbf{N}, b \in \mathbf{N}^*, \dot{(a, b)} \in \frac{\mathbf{Z} \times \mathbf{Z}^*}{\mathrm{R}} \right\}$$

ou encore :

$$\mathbf{Q}'' = \left\{ \dot{(a, b)} \; ; \dot{(a, b)} \in \frac{\mathbf{Z} \times \mathbf{Z}^*}{\mathrm{R}}, ab \geqslant 0 \right\}.$$

Or, $\mathbf{Q}''$ a pour Q les propriétés d'un G+. En effet :

$$\mathbf{Q}'' + \mathbf{Q}'' = \mathbf{Q}''.$$

D'autre part $\mathbf{Q}''^-$, ensemble des opposés des éléments de $\mathbf{Q}''$, peut être considéré comme l'ensemble des classes de $\frac{\mathbf{Z} \times \mathbf{Z}^*}{\mathrm{R}}$ où $ab \leqslant 0$;

donc :

$$\mathbf{Q}'' \cap \mathbf{Q}''^- = \{0\}.$$

$\mathbf{Q}''$ permet donc de définir sur **Q** une relation d'ordre total :

$$x > y \Longleftrightarrow x - y \in \mathbf{Q}''.$$

En particulier si $x = \dot{(a, b)}$ et $y = \dot{(c, b)}$:

$$x > y \Longleftrightarrow \dot{(a - c, b)} \in \mathbf{Q}'' \Longleftrightarrow (a - c)b \geqslant 0,$$

ce qui revient à dire que pour comparer deux éléments de **Q** on peut choisir des représentants de la classe ayant même dénominateur positif et comparer les numérateurs.

Remarque importante : Il faut noter que la relative complication de cette théorie vient de ce que nous avons voulu montrer que les définitions adoptées pour les opérations étaient les seules possibles. Il est bien évident qu'on obtiendrait, à l'usage des élèves, une théorie beaucoup plus simple en posant au départ ces définitions et en établissant ensuite leurs propriétés.

Exercice 36.

Soit x un élément quelconque de E et $1x$ son produit par 1. Considérons la différence :

$$x_2 = x - 1x$$

et formons son produit par 1. Il vient :

$$1x_2 = 1x - 1(1x) = 1x - 1x = 0$$

donc :

$$1x_2 = 0 \qquad x_2 \in E_2$$

et x s'écrit :

$$x = x_2 + x_1$$

en posant $1x = x_1$. Or $1(1x) = 1x$, donc $x_1 \in E_1$.

Pour montrer que E est la somme directe de E_1 et E_2 il suffit de montrer que E_1 et E_2 sont des sous-groupes. En effet E étant commutatif la permutabilité est automatique. D'autre part il est clair que 0 est le seul x tel que $1x = x$ et $1x = 0$, ce qui entraîne $E_1 \cap E_2 = \{0\}$, condition suffisante pour que la somme $E_1 + E_2$ soit directe (II, 3, 2).

Or E_1 est bien un sous-groupe car :

1) $\left.\begin{matrix} 1x_1 = x_1 \\ 1x'_1 = x'_1 \end{matrix}\right\} \Rightarrow 1(x_1 + x'_1) = x_1 + x'_1 \Rightarrow x_1 + x'_1 \in E_1,$

2) $1x_1 + 1(-x_1) = 1(x_1 + (-x_1)) = 0 \Rightarrow 1(-x_1) = -1x_1 = -x_1 \Rightarrow -x_1 \in E_1,$

et E_2 est bien un sous-groupe, car :

1) $\left.\begin{matrix} 1x_2 = 0 \\ 1x'_2 = 0 \end{matrix}\right\} \Rightarrow 1(x_2 + x'_2) = 0 \Rightarrow x_2 + x'_2 \in E_2,$

2) $1x_2 + 1(-x_2) = 1[x_2 + (-x_2)] = 0 \Rightarrow 1(-x_2) = 0 \Rightarrow -x_2 \in E_2.$

On peut donc conclure :

$$E = E_1 \oplus E_2$$

E_1 étant un sous-groupe pour lequel l'opération induite par l'opération définie sur E, satisfait à tous les axiomes de la structure d'espace vectoriel, est bien un espace vectoriel.

Exercice 37.

Soient f et g deux applications de E dans H. On peut définir l'application $f + g$ par :

$$\forall x \in E \qquad (f + g)(x) = f(x) + g(x).$$

le $+$ du 2e membre étant le signe de l'opération interne sur H et celui du premier membre celui de l'opération ainsi définie sur $\mathcal{F}$.

Si H *est un groupe*, $\mathcal{F}$ est aussi un groupe. En effet, la loi de composition ci-dessus définie est associative si celle de H l'est. Cette loi de composition admet un élément neutre, l'application ε telle que :

$$\forall x \in E \qquad \varepsilon(x) = 0.$$

Enfin, chaque élément f a un inverse $-f$ défini par :

$$\forall x \in E \qquad [-f](x) = -f(x).$$

Considérons alors l'application :

$$h_x : \mathcal{F} \to H \qquad h_x(f) = f(x)$$

où x est un élément fixe de E. L'ensemble $\mathcal{F}$ étant doté de la loi de composition définie ci-dessus, l'égalité de définition montre que cette application est un homomorphisme. Le noyau de l'homomorphisme est l'ensemble $\mathcal{F}_x$ des applications f telles que $f(x) = 0$ et, dans une même classe, modulo $\mathcal{F}_x$, nous trouvons toutes les fonctions qui prennent la même valeur pour la valeur x. [Tout ceci a d'ailleurs été dit dans le cours (II, 2, 8, IV), dans le cas où E était un sous-ensemble de **R** et l'ensemble des applications étant limité à celles qui étaient continues].

Si H *est anneau* nous définissons de même :

$$\forall x \in E \qquad [fg](x) = f(x)\, g(x)$$

et nous vérifions que la nouvelle loi de composition est associative et qu'elle est distributive par rapport à la première, toutes les égalités à vérifier sur f, g, h se traduisant par des égalités de forme identique sur $f(x)$, $g(x)$, $h(x)$, vraies pour tout x.

Les applications h_x considérées ci-dessus seraient alors des homomorphismes d'anneau.

Enfin si H *est un corps* nous pourrons bien définir un élément neutre pour la deuxième loi de composition sur $\mathcal{F}$: l'application η telle que :

$$\forall x \in E \qquad \eta(x) = 1$$

mais quand nous voudrons trouver f^{-1} telle que $ff^{-1} = \eta$, f étant différent de ε, nous verrons que f^{-1} n'existe pas nécessairement car il faudrait avoir :

$$\forall x \in E \qquad f^{-1}(x) = \frac{1}{f(x)}.$$

Or $f(x)$ peut être égal à 0 pour certaines valeurs de x. $\mathcal{F}$ n'est donc pas un corps.

2) Nous définissons λf par :

$$\forall x \in E \qquad (\lambda f)(x) = \lambda f(x).$$

Si H a une structure d'espace vectoriel sur le corps K des opérateurs λ, on vérifie immédiatement que si e est l'élément unitaire de K, ef est définie par :

$$\forall x \in E \qquad (ef)(x) = ef(x) = f(x)$$

donc :

$$\forall f \in \mathcal{F} \qquad ef = f.$$

$\lambda\mu f$ est définie par :

$$\forall x \in E \qquad (\lambda\mu f)(x) = \lambda\mu f(x) = \lambda(\mu f)(x)$$

donc :

$$(\lambda\mu)f = \lambda(\mu f).$$

$(\lambda + \mu)f$ est définie par :

$$\forall x \in E \quad [\lambda + \mu)f](x) = (\lambda + \mu)f(x) = \lambda f(x) + \mu f(x) = (\lambda f)(x) + (\mu f)(x)$$

donc :

$$(\lambda + \mu)f = \lambda f + \mu f.$$

$\lambda(f + g)$ est définie par :

$$\forall x \in E \qquad [\lambda(f + g)](x) = \lambda(f + g)(x) = \lambda[f(x) + g(x)] = \lambda f(x) + \lambda g(x) = (\lambda f)(x) + (\lambda g)(x)$$

donc :

$$\lambda(f + g) = \lambda f + \lambda g.$$

$\mathcal{F}$ vérifie donc les axiomes de la structure d'espace vectoriel sur K.

3) Soit $\prec$ l'ordre sur H. Nous pourrons poser :

$$\forall x \in E \qquad f \prec g \Longleftrightarrow f(x) \prec g(x).$$

Il est immédiat que les trois axiomes d'une structure d'ordre sont vérifiés. Mais si E a au moins deux éléments x et y les applications f et g telles que :

$$f(x) \prec g(x) \qquad g(y) \prec f(y)$$

ne sont pas comparables. $\mathcal{F}$ n'aura donc jamais une structure d'ordre total.

Si H *est un treillis* nous pourrons définir l'inf et le sup de f et g par :

$$\forall x \in E \qquad [f \wedge g](x) = f(x) \wedge g(x)$$
$$\forall x \in E \qquad [f \vee g](x) = f(x) \vee g(x)$$

et $\mathcal{F}$ sera aussi un treillis.

4) Nous définirons une relation S sur $\mathcal{F}$ par :

$$\forall x \in E \qquad fSg \Longleftrightarrow f(x)Rg(x).$$

On vérifie immédiatement que S est réflexive, symétrique et transitive. S est une relation d'équivalence. Dans une même classe modulo S nous trouvons les applications qui font correspondre à un même élément de E des éléments de H équivalents (mod R). A toutes les applications d'une même classe de $\mathcal{F}$ (mod S) correspond donc une application de E dans H/R. L'ensemble des applications de :

$$E \longrightarrow H/R$$

est donc isomorphe à $\mathcal{F}/S$.

Exercice 38.

Soit A un anneau d'intégrité fini à n éléments et soit $a \neq 0$ appartenant à A. Considérons tous les produits xa. Nous pouvons affirmer que :

$$x \neq x' \Rightarrow xa \neq x'a.$$

En effet $xa = x'a$ entraînerait $(x - x')a = 0$, soit $x = x'$. Les produits xa tous différents sont donc égaux aux $n - 1$ éléments non nuls de A et l'équation $xa = b$ a une solution pour tout $b \in A$. On montrerait de la même façon en considérant les produits à droite que $ax = b$ a une solution pour tout b. $A - \{0\}$ est donc un groupe multiplicatif (cf. cours II, 2, 2), donc A est un corps.

Exercice 39.

Soient deux polynômes :

$$P = [a_0, a_1 \ldots\ldots a_m]$$
$$Q = [b_0, b_1 \ldots\ldots b_n]$$

appartenant à $A[x]$ et dont le produit est nul.

$$PQ = 0, \text{ c'est-à-dire } \begin{cases} a_0b_0 = 0 \\ a_0b_1 + a_1b_0 = 0 \\ a_0b_2 + a_1b_1 + a_2b_0 = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0b_p + a_1b_{p-1} + \ldots\ldots + a_pb_0 = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{cases}$$

et supposons que Q soit différent de 0. Nous allons montrer qu'on pourra en conclure que $P = 0$ si A est un anneau d'intégrité.

Soit en effet b_λ le premier des coefficients différents de 0 de Q. Pour que :

$$a_0b_\lambda + a_1b_{\lambda-1} + \ldots\ldots + a_\lambda b_0 = 0$$

il faut que :

$$a_0b_\lambda = 0 \qquad \text{donc : } a_0 = 0.$$

Mais alors la nullité du coefficient suivant de PQ :

$$a_0b_{\lambda+1} + a_1b_\lambda + \ldots\ldots + a_{\lambda+1}b_0$$

entraîne :

$$a_1b_\lambda = 0 \qquad \text{donc : } a_1 = 0$$

et ainsi de suite. Quand on aura montré que tous les a_i sont nuls jusqu'à l'indice μ on considérera le coefficient d'indice $\lambda + \mu + 1$ de PQ :

$$\underbrace{a_0b_{\lambda+\mu+1} + \ldots\ldots + a_\mu b_{\lambda+1}}_{\text{tous les } a \text{ sont nuls}} + a_{\mu+1}b_\lambda + \underbrace{a_{\mu+2}b_{\lambda-1} + \ldots\ldots + a_{\lambda+\mu+1}b}_{\text{tous les } b \text{ sont nuls}}$$

et sa nullité entraînera :

$$a_{\mu+1}b_\lambda = 0 \qquad \text{donc : } a_{\mu+1} = 0.$$

Tous les coefficients de P sont donc nuls.

Si au contraire A n'est pas un anneau d'intégrité, $A[x]$ n'en sera pas un. C'est évident car il suffit de considérer les deux polynômes :

$$[a, 0, 0 \ldots\ldots] \quad \text{et} \quad [b, 0, 0 \ldots\ldots]$$

où a et b représentent des diviseurs de zéro de A ($a \neq 0$, $b \neq 0$, $ab = 0$). Le produit de ces deux polynômes est nul. L'anneau $A[x]$ possède d'ailleurs des diviseurs de zéro plus intéressants. Un polynôme dont tous les coefficients sont multiples de 3 (sans l'être de 6) sera un diviseur de 0 dans $\mathbf{Z}_6[x]$, anneau des polynômes dont les coefficients sont des entiers modulo 6.

Exercice 40 (sur les anneaux de Boole).

1) Evaluons $(a + a)^2$. L'hypothèse entraîne $(a + a)^2 = a + a$. Mais si nous calculons le carré de la somme $a + a$ en utilisant la distributivité, il vient aussi :

$$(a + a)^2 = a^2 + a^2 + a^2 + a^2 = a + a + a + a$$

donc :

$$a + a = a + a + a + a \qquad \text{soit : } a + a = 0.$$

2) Evaluons maintenant $(a + b)^2$. On trouve de même :

$(a + b)^2 = a + b$ et $(a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$

D'où : $a + b = a + ab + ba + b$

$ab + ba = 0$

mais en vertu du 1) : $ab + ab = 0$

le rapprochement des deux égalités donne :

$$\forall (a, b) \in A^2 \qquad ab = ba$$

et A est commutatif.

3) Supposons que A possède au moins trois éléments ; deux d'entre eux a et b sont différents de zéro et distincts. Calculons :

$$ab(a + b) = aba + abb = a^2b + ab^2 = ab + ab = 0.$$

Or par hypothèse $a \neq 0$, $b \neq 0$ et $a + b \neq 0$ (car $a + b = 0$ entraînerait $a + b = a + a$, donc $a = b$, ce qui est contraire à l'hypothèse). Donc $ab(a + b)$ est nul sans que ni a, ni b, ni $a + b$ le soit ; alors, ou bien $ab \neq 0$ et ab et $a + b$ sont des diviseurs de zéro, ou bien $ab = 0$ et a et b sont des diviseurs de zéro.

4) En fait $a + b$ qui n'est pas nul ne peut non plus être égal à a (ce qui entraînerait $b = 0$), ni à b ; $a + b$ est donc un 4e élément distinct de a, b, 0. Et un anneau de Boole qui a plus de deux éléments en a au moins quatre. Il est d'ailleurs facile de vérifier à l'aide des tables de groupes (corrigé exercice 19) que l'unique table de groupe à trois éléments ne saurait être une table de groupe additif d'anneau de Boole, car les éléments de sa diagonale principale ($a + a$, $b + b$) ne sont pas nuls.

Les structures d'anneaux de Boole les plus simples que nous trouvons sont donc les suivantes :

1) $n = 2$. Les tables d'addition et de multiplication sont les suivantes :

	0	a
0	0	a
a	a	0

	0	a
0	0	0
a	0	a

Cette structure est d'ailleurs l'unique structure d'anneau (ou de corps) à deux éléments. Elle est isomorphe à celle de l'ensemble des par-

ties d'un ensemble à un élément α, muni des lois de composition, différence symétrique et intersection.

[Dans le tableau ci-dessus 0 représente la partie vide et a la partie $\{\alpha\}$].

2) $n = 4$. En nous reportant aux tables de groupes (exercice 19) nous voyons que seule la première peut convenir pour la première opération. Pour la 2° opération la propriété $a^2 = a$ et la commutativité nous impose déjà plusieurs résultats. On a donc :

addition	0	a	b	c
0	0	a	b	c
a		0	c	b
b			0	a
c				0

multiplication	0	a	b	c
0	0	0	0	0
a		a		
b			b	
c				c

Nous pouvons avoir *a priori* $ab = 0$ et $ab = a$ (ou $ab = b$, mais ceci ne constitue pas deux cas distincts) et $ab = c$. Mais on élimine tout de suite ce dernier cas, car $c = a + b$ et le raisonnement précédent a prouvé que $ab(a + b) = 0$, ce qui donnerait $c^2 = 0$, ce qui est impossible.

Si on prend $ab = 0$ la distributivité nous fournira :

$$ac = a(a + b) = a^2 + ab = a$$
$$bc = b(a + b) = ba + b^2 = b$$

et la table de 2° opération sera :

	0	a	b	c
0	0	0	0	0
a		a	0	a
b			b	b
c				c

Si on prend $ab = a$ la distributivité nous fournit :

$$ac = a(a + b) = a^2 + ab = a + a = 0$$
$$bc = b(a + b) = ba + b^2 = a + b = c$$

et on voit que, par rapport au cas précédent, il y a seulement échange des rôles joués par b et c.

Nous avons donc une seule structure d'anneau de Boole à quatre éléments. Cet anneau est isomorphe à l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble à deux éléments α et β ; on aura la partie vide 0, les parties $\{\alpha\}$ et $\{\beta\}$ qui jouent les rôles de a et b et l'ensemble E lui-même qui joue le rôle de c ($\{\alpha\} \Delta \{\beta\} = E$, $\{\alpha\} \cap \{\beta\} = 0$).

Exercice 41.

On peut soit refaire sur cet exemple le raisonnement fait ci-dessus (ex. 38) et on reconnaîtra la démonstration classique conduisant au théorème de Fermat, soit appliquer le résultat de cet exercice :

L'anneau $\mathbf{Z}_m$ des entiers naturels modulo m est un anneau d'intégrité ; en effet, si m est premier on ne peut avoir :

$$\dot{p}\dot{q} = 0 \qquad \text{c'est-à-dire } m|pq$$

sans que $m|p$ (ou $m|q$), c'est-à-dire $\dot{p} = 0$ (ou $\dot{q} = 0$), $\mathbf{Z}_m$ est donc un corps si m est premier.

Si m n'est pas premier il est clair que $\mathbf{Z}_m$ admet des diviseurs de zéro, donc n'est pas un corps.

Exercice 42.

On vérifie immédiatement que le polynôme $x^2 + 1$ n'admet aucun diviseur autre que 1 dans $\mathbf{Z}[x]$. Si donc $x^2 + 1$ et $2x$ appartenait à un même idéal principal ce ne pourrait être que l'idéal (1), c'est-à-dire l'anneau tout entier. Or, ceci est impossible ; en effet tous les éléments de l'idéal $(x^2 + 1, 2x)$ étant de la forme :

$$\lambda(x)\,(x^2 + 1) + \mu(x) \times 2x$$

il est clair que les seuls polynômes du premier degré présents parmi eux seront de la forme $2px$. L'idéal ne contient donc pas l'anneau tout entier.

Exercice 43.

D'après la construction d'un idéal principal dans un anneau sans élément unité l'idéal principal (4) est l'ensemble :

$$\{\, 4n + 4 \times 2m \ ;\ n \in \mathbf{Z},\ 2m \in \mathrm{A} \,\}$$

c'est-à-dire l'ensemble des multiples entiers de 4, soit 4Z.

(4)A apparaît alors comme l'ensemble des multiples entiers de 8, donc l'inclusion :

$$(4)\mathrm{A} \subset \mathrm{A}$$

est stricte.

(4)A est bien un idéal I, puisque la différence de deux multiples de 8 est un multiple de 8 et que le produit d'un multiple de 8 par un élément de A est encore un multiple de 8. Mais un tel multiple est en outre un multiple entier de 16 et AI, ensemble des multiples entiers de 16, est inclus strictement dans I.

Exercice 44.

1) La définition de l'idéal primaire se traduit par la propriété suivante relative aux éléments de A/I :

$$\left.\begin{array}{l} \dot{a}\dot{b} = 0 \\ \dot{a} \neq 0 \end{array}\right\} \Rightarrow \quad \exists\, \rho \in \mathbf{N} \qquad \widehat{\dot{b}^{\rho}} = 0$$

Mais en vertu de l'homomorphisme $\mathrm{A} \longrightarrow \mathrm{A/I}$:

$$\widehat{\dot{b}^{\rho}} = (\dot{b})^{\rho}$$

donc :

$$\left.\begin{array}{l} \dot{a}\dot{b} = 0 \\ \dot{a} \neq 0 \end{array}\right\} \Rightarrow \quad \exists\, \rho \in \mathbf{N} \qquad (\dot{b})^{\rho} = 0$$

c'est la propriété énoncée.

2) Soient a et b appartenant à J :

$$a \in \mathrm{J} \Longleftrightarrow \quad \exists \rho \in \mathbf{N} \qquad a^{\rho} \in \mathrm{I}$$
$$b \in \mathrm{J} \Longleftrightarrow \quad \exists \rho' \in \mathbf{N} \qquad b^{\rho'} \in \mathrm{I}$$

Nous devons montrer que $a - b \in \mathrm{J}$ et que pour tout $x \in \mathrm{A}$, $xa \in \mathrm{J}$, $ax \in \mathrm{J}$.

a) Considérons :

$$(a - b)^{\rho+\rho'} = \Sigma\, (-1)^{\lambda}\, C^{\lambda}_{\rho+\rho'}\ a^{\lambda}\, b^{\mu}$$
$$\text{avec } \mu = \rho + \rho' - \lambda.$$

Si $\lambda > \rho$, a^{λ} multiple de a^{ρ} appartient à I.

Si $\lambda < \rho$, il en résulte $\mu > \rho'$ et b^{μ}, multiple de $b^{\rho'}$, appartient à I, donc tous les termes du développement précédent appartiennent à I et $(a - b)^{\rho+\rho'} \in \mathrm{I}$, ce qui entraîne :

$$a - b \in \mathrm{J}.$$

b) $\quad (xa)^{\rho} = x^{\rho}a^{\rho} \in \mathrm{I} \quad$ donc $\quad xa \in \mathrm{J}$,
$\quad (ax)^{\rho} = a^{\rho}x^{\rho} \in \mathrm{I} \quad$ donc $\quad ax \in \mathrm{J}$.

D'autre part, il est clair que les éléments de I appartiennent à J.

Montrons enfin que J est un idéal premier. Soient donc :

$$ab \in J \qquad a \notin J$$

la première partie de l'hypothèse se traduit par :

$$\exists \rho \in N \qquad (ab)^\rho = a^\rho b^\rho \in I$$

or, la 2e partie de l'hypothèse donne : $a^\rho \notin I$.

Le fait que I soit primaire entraîne alors :

$$\exists \lambda \in N \qquad (b^\rho)^\lambda \in I$$

mais $(b^\rho)^\lambda = b^{\rho\lambda}$ donc $b^{\rho\lambda} \in I \Rightarrow b \in J$.

En définitive :

$$\left.\begin{array}{l} ab \in J \\ a \notin J \end{array}\right\} \Rightarrow b \in J$$

ce qu'on voulait démontrer.

Exercice 45.

La classe d'équivalence d'un polynôme $P(x)$ $(\mathrm{mod}\, x^2+1)$ est l'ensemble :

$$P(x) + \lambda(x)\,(x^2+1)$$

où $\lambda(x)$ décrit $\mathbf{Z}[x]$. On peut prendre comme représentant de la classe le reste de la division de $P(x)$ par x^2+1 (division définie dans $\mathbf{R}[x]$, mais qui donne pour reste un polynôme à coefficients entiers quand P est à coefficients entiers).

L'anneau quotient :

$$\mathbf{Z}[x]/(x^2+1)$$

(x^2+1) désignant l'idéal engendré par x^2+1 est alors un anneau d'intégrité car on ne peut trouver deux polynômes du premier degré différents de zéro dont le produit soit dans l'idéal, ce qui exigerait que ce produit soit x^2+1. (x^2+1) est donc un idéal premier.

Il n'est pas maximal. Il suffit de se reporter à l'exercice 42, où nous avons vu que l'idéal engendré par x^2+1 et $2x$, idéal qui contient évidemment (x^2+1), n'était pas l'anneau $\mathbf{Z}[x]$ tout entier.

Exercice 46.

1) Soit un idéal de $2\mathbf{Z}$ et soit $2m$ le plus petit de ses éléments $\neq 0$. Soit $2n$ un autre de ses éléments. Ecrivons :

$$\begin{array}{ll} n = mp + r & r < m \\ 2n = 2mp + 2r & 2r < 2m \end{array}$$

$2r$ devrait appartenir à l'idéal, ce qui est contraire à l'hypothèse si $r \neq 0$. Donc $2n$ est multiple de $2m$ et l'idéal est principal.

2) L'idéal $(2m)$ est maximal s'il n'existe aucun idéal différent de $2\mathbf{Z}$ qui le contienne, ce qui exige donc qu'il n'existe pas $2p$ tel que :

$$(2p) \supset (2m) \qquad \text{ou} \quad 2p \mid 2m \qquad p \mid m.$$

Il faut donc (et il suffit) que m soit premier.

L'anneau quotient $2\mathbf{Z}/(2m)$ est formé des classes d'entiers congrus à $2n$ modulo $2m$, n prenant les valeurs $0, 1, \ldots, m-1$.

Dire que cet anneau possède des diviseurs de zéro, c'est dire qu'il existe p et q n'appartenant pas à $(2m)$:

$$m \text{ ne divise pas } p, \quad m \text{ ne divise pas } q$$

tels que :

$$2p \times 2q \in (2m)$$

donc :

$$2m \mid 2p \times 2q \qquad m \mid 2pq$$

m étant premier cela entraîne $m \mid 2$, donc $m = 2$.

Le seul idéal maximal de $2\mathbf{Z}$ tel que l'anneau quotient possède des diviseurs de 0 est l'idéal (4).

L'anneau quotient est un anneau à deux éléments :

$$(\dot 0 \text{ et } \dot 2) \text{ et } \dot 2 \times \dot 2 = \dot 0$$

(en d'autres termes : $(4\lambda+2)(4\mu+2) = 4\nu$).

Nous avons ici un exemple d'idéal maximal tel que l'anneau quotient ne soit pas un corps. Ceci tient au fait que $2\mathbf{Z}$ ne possède pas d'élément unité.

Exercice 47.

1) La définition des opérations montre que $\mathcal{A}$ est un groupe additif dont l'élément neutre est le polynôme nul ($\forall r \quad a_r = 0$).

Elle montre aussi que la multiplication est commutative puisque celle de A l'est. Vérifions que cette multiplication est associative.

$$[\,|\,a_r\,|\;|\,b_r\,|\,]\,|\,c_r\,| = \left\{ \sum_{s+t=r} a_s b_t \right\} |\,c_r\,| = \left\{ \sum_{s+t+u=r} a_s b_t c_u \right\}.$$

Il est clair qu'on aurait trouvé le même résultat pour :

$$|\,a_r\,|\,[\,|\,b_r\,|\;|\,c_r\,|\,]$$

Vérifions que cette multiplication est distributive par rapport à l'addition :

$$|\,a_r\,|\,[\,|\,b_r\,| + |\,c_r\,|\,] = |\,a_r\,|\;|\,b_r + c_r\,| = \left\{ \sum_{s+t=r} a_s (b_t + c_t) \right\}$$

$$= \left\{ \sum_{s+t=r} a_s b_t + a_s c_t \right\}$$

Or :

$$|\,a_r\,|\;|\,b_r\,| + |\,a_r\,|\;|\,c_r\,| = \left\{ \sum_{s+t=r} a_s b_t \right\} + \left\{ \sum_{s+t=r} a_s c_t \right\}$$

$$= \left\{ \sum_{s+t=r} a_s b_t + a_s c_t \right\}.$$

$\mathcal{A}$ est donc bien un anneau commutatif. Cet anneau ne possède pas d'élément unité. En effet si ρ est le plus petit des indices r d'un polynôme P, le plus petit des indices du polynôme produit de P par un polynôme quelconque Q sera supérieur à ρ puisque les indices r sont strictement positifs. Donc il ne peut exister de polynôme Q tel que $PQ = P$.

2) Si un idéal contient x^r il contient x^s pour tout $s > r$ puisque x^s est le produit de x^r par x^{s-r} qui est un élément de $\mathcal{A}$.

3) Si un idéal $\mathcal{I}$ contient x^r quel que soit r, c'est $\mathcal{A}$ tout entier. En effet, tout polynôme P peut se mettre sous la forme $x^r Q$ par la mise en facteur d'un monôme de degré inférieur à celui de son terme de plus bas degré. P appartiendrait donc à $\mathcal{I}$.

Etant donné un idéal $\mathcal{I} \neq \mathcal{A}$ il existe donc une valeur r telle que :

$$x^r \notin \mathcal{I}$$

et alors $x^{r-h} \notin \mathcal{I}$ pour tout h rationnel positif (car $x^{r-h} \in \mathcal{I}$ entraînerait $x^r \in \mathcal{I}$ en vertu de 2).

Si d'autre part il existe dans l'idéal J un monôme $x^{r'}$:

$$\forall h \text{ rationnel} > 0 \qquad x^{r'+h} \in \mathcal{J}.$$

Il résulte de ceci qu'on peut faire parmi les rationnels une coupure en mettant :

dans la 1re classe tous les r tels que $x^r \notin \mathcal{J}$

dans la 2e ..... $x^r \in \mathcal{J}$

tout rationnel est classé et tout nombre de la première classe est inférieur à tout nombre de la deuxième.

Cette coupure définit un nombre r_0 et :

$$\forall r > r_0 \qquad x^r \in \mathcal{J}$$
$$\forall r < r_0 \qquad x^r \notin \mathcal{J}.$$

Ceci posé considérons un idéal $\mathcal{J} \neq A$ qui contient un monôme de coefficient 1 et pour lequel, en conséquence, le raisonnement précédent s'applique. Nous allons montrer que cet idéal n'est contenu dans aucun idéal maximal.

Supposons qu'il soit contenu dans un tel idéal $\mathcal{J}' \supset \mathcal{J}$. Le raisonnement précédent s'applique encore et on peut pour $\mathcal{J}'$ définir r_0. Soit alors :

$$r_1 < r_0 \Rightarrow x^{r_1} \notin \mathcal{J}'.$$

Si $\mathcal{J}'$ était maximal l'idéal $\mathcal{J}''$ engendré par x^{r_1} et $\mathcal{J}'$ devrait être $\mathcal{A}$ tout entier. Or :

$$\mathcal{J}'' = x^{r_1}\mathcal{A} + \mathcal{J}'$$

considérons :

$$x^{r_2} \qquad \text{avec } r_2 < r_1 < r_0.$$

Si x^{r_2} appartenait à $\mathcal{J}''$ c'est qu'il existerait dans $\mathcal{J}'$ un polynôme Q tel que :

$$x^{r_2} = x^{r_1} P + Q.$$

Multiplions alors cette égalité par x^ρ, ρ étant choisi de façon à ce que :

$$r_2 + \rho < r_0 < r_1 + \rho.$$

Nous aboutissons à une contradiction car :

$$x^{r_1+\rho} \in \mathcal{J}' \qquad Qx^\rho \in \mathcal{J}'$$

alors que :

$$x^{r_2+\rho} \notin \mathcal{J}'.$$

Nous en concluons que x^{r_2} ne peut appartenir à $\mathcal{J}''$ qui n'est donc pas $\mathcal{A}$ tout entier. $\mathcal{J}'$ n'est donc pas maximal et $\mathcal{J}$ n'est inclus dans aucun idéal maximal.

Exercice 48.

1) L'image réciproque d'un sous-groupe dans un homomorphisme de groupe est un sous-groupe. Nous avons déjà eu, par exemple, l'occasion de la montrer dans l'exercice 23.

Il reste si l'on pose :

$$I_1 = \overset{-1}{f}(I_2)$$

à vérifier que :

$$\forall a_1 \in A_1 \qquad a_1 I_1 \subset I_1 \qquad I_1 a_1 \subset I_1.$$

Or :

$$f(a_1 I_1) = f(a_1)\, f(I_1) \subset f(a_1) I_2 \subset I_2$$
$$f(I_1 a_1) = f(I_1)\, f(a_1) \subset I_2 f(a_1) \subset I_2$$

puisque I_2 est un idéal bilatère de A_2.

I_1 est donc un idéal bilatère de A_1.

Si en particulier on considère l'injection canonique :

$$A_1 \longrightarrow A_2$$

faisant correspondre à lui-même tout élément de A_1, l'image réciproque de I_2 est $A_1 \cap I_2$ qui est donc un idéal bilatère de A_1 (cette propriété se démontre d'ailleurs sans peine directement).

Considérons les applications suivantes :

$$\begin{array}{ccc} A_1 & \xrightarrow{\ f\ } & A_2 \\ \varphi_1 \downarrow & & \downarrow \varphi_2 \\ A_1/I_1 & & A_2/I_2 \end{array}$$

1) Si f est un homomorphisme surjectif l'application $\varphi_2 \circ f = g$, produit de deux homomorphismes surjectifs, est un homomorphisme surjectif. D'après le théorème général, A_2/I_2 est donc isomorphe à l'anneau quotient de A_1 par l'idéal $\overset{-1}{g}(0)$, 0 étant l'élément neutre de l'addition sur l'anneau A_2/I_2 (voir cours page 66). Or l'élément neutre de cette addition, c'est la classe neutre de $A_2 \pmod{I_2}$, $\overset{-1}{\varphi_2}(0) = I_2$, et comme $\overset{-1}{f}(I_2) = I_1$,

$$\overset{-1}{g}(0) = I_1.$$

On a donc :

$$A_2/I_2 \approx A_1/I_1.$$

Remarque. Ce raisonnement est l'exacte répétition au cas des anneaux de celui fait dans l'exercice cité ci-dessus, dans le cas des groupes.

Il aurait suffi à établir à lui seul, dans le cas où f est surjectif, que I_1 étant $\overset{-1}{g}(0)$, donc le noyau d'un homomorphisme d'anneaux, était un idéal bilatère.

2) Si maintenant f n'est plus surjectif le raisonnement ci-dessus ne s'applique plus à A_2, mais considérons :

$$f(A_1) = A'_2$$

A'_2 est un sous-anneau de A_2 ; d'après ce qui a été dit ci-dessus :

$$I_2 \cap A'_2 = I'_2$$

est un idéal bilatère de A'_2 dont l'image réciproque par f est I_1. f considérée comme application de A_1 sur A'_2 :

$$A_1 \xrightarrow{\ f\ } A'_2$$

est, elle, un homomorphisme surjectif auquel s'applique le raisonnement précédent et nous pouvons dire que :

$$A_1/I_1 \approx A'_2/I'_2.$$

Cet isomorphisme :

$$A_1/I_1 \xrightarrow{\ \psi\ } A'_2/I'_2$$

fait correspondre :

$$\dot{a}_1 \longrightarrow f(a_1)$$

avec :

$$f(\dot{a}_1) = f(a_1 + I_1) = a_2 + I'_2 = a_2 + I_2 \cap A'_2.$$

Or tout x appartenant à $a_2 + I_2 \cap A'_2$ appartient à A'_2 (puisque somme de deux éléments appartenant à A'_2). Il appartient aussi à $a_2 + I_2$; donc :

$$a_2 + I_2 \cap A'_2 \subset (a_2 + I_2) \cap A'_2.$$

Mais, réciproquement, soit y appartenant au deuxième membre de cette formule : $y \in A'_2$, $a_2 \in A'_2$, donc $y - a_2 \in A'_2$; d'autre part :

$y - a_2 \in I_2 \cap A'_2$ et $y \in a_2 + I_2 \cap A'_2$. On a donc :

$$a_2 + I_2 \cap A'_2 = (a_2 + I_2) \cap A'_2 = \dot{a}_2 \cap A'_2$$

et : $$f(\dot{a}_1) = \dot{a}_2 \cap A'_2.$$

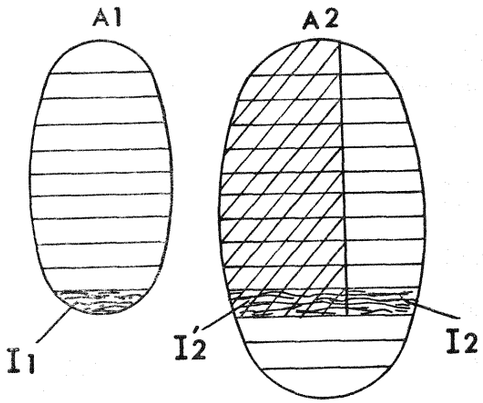
Chaque classe de A'_2 (mod I'_2) est donc l'intersection de A'_2 avec une classe de A_2 (mod I_2).

Il existe donc une bijection entre les classes de A_1 (mod I_1) et celles des classes de A_2 (mod I_2) dont l'intersection avec A'_2 n'est pas vide. Cette bijection est un isomorphisme puisque ψ en est un et que la composée de deux classes de A_2 (par addition ou multiplication) est la classe obtenue en faisant les opérations sur les classes de A'_2 incluses dans ces classes.

Si maintenant nous considérons toutes les classes de A_2 (mod I_2) l'application :

$$A_1/I_1 \longrightarrow A_2/I_2$$

n'est plus un isomorphisme puisque les classes de A_2 dont l'intersection avec A'_2 est vide ne sont pas obtenues dans cette application, mais, en vertu de ce qui précède, elle est un *homomorphisme injectif*.



Le dessin ci-contre schématise les partitions de A_1 (mod I_1) et celles de A_2 (mod I_2) et de A'_2 (hachuré obliquement) (mod I'_2).

2) Supposons que A_1/I_1 admette des diviseurs de zéro, $\dot{a}_1$ et $\dot{b}_1$, c'est-à-dire :

$$\exists\, a_1 \in A_1,\ b_1 \in A_1\ a_1 \notin I_1 \quad b_1 \notin I_1\ a_1 b_1 \in I_1$$

pour leurs homologues a_2 et b_2 il en résulterait :

$$a_2 b_2 \in I_2$$

I_2 étant premier ceci exige : $a_2 \in I_2$ si $b_2 \notin I_2$. Mais si $a_2 \in I_2$:

$$a_1 \in \overline{f}^{1}(I_2) = I_1$$

ce qui est contraire à l'hypothèse.

A_1/I_1 n'admet donc pas de diviseurs de zéro et I_1 est premier.

Exercice 49.

1) $Aa = \mathcal{I}$ est un idéal à gauche ; en effet :

$$xa - ya = (x - y)a \in \mathcal{I},$$
$$y(xa) = (yx)a \in \mathcal{I}.$$

2) Dire que A n'est pas un anneau de carré nul, c'est dire qu'il existe au moins un élément a tel que $Aa \neq \{0\}$ (sans quoi on aurait $ba = 0$ $\forall a,\ \forall b \in A$). Mais d'après 1) Aa est un idéal à gauche, l'hypothèse entraîne alors que :

$$Aa = A$$

c'est-à-dire que quand x décrit A, xa décrit A. Il existe donc un élément e tel que :

$$ea = a.$$

Considérons alors l'ensemble :

$$I = \{ x - xe\ ;\ x \in A \}$$
$$(x - xe) - (y - ye) = x - y - (x - y)e \in I$$
$$y(x - xe) = yx - (yx)e \in I,$$

I est donc un idéal à gauche ; donc $I = A$ ou $I = \{0\}$.

Mais si on avait $I = A$ on aurait $Ia = Aa = A$.

Or :

$$Ia = \{ xa - xea\ ;\ x \in A \} = \{0\}.$$

Il y a donc contradiction et :

$$I = \{0\}.$$

C'est-à-dire que :

$$\forall x \in A \qquad x = xe \tag{1}$$

Soit maintenant

$$J = \{ x - ex\ ;\ x \in A \}$$
$$(x - ex) - (y - ey) = (x - y) - e(x - y) \in J$$
$$y(x - ex) = yx - yex$$

mais en vertu de (1) :

$$y = ye \quad \text{et} \quad y(x - ex) = 0 \in J$$

ce qui montre que J est un idéal à gauche et signifie en outre que $AJ = 0$. Si donc on avait $J = A$ on aurait $A^2 = 0$, contrairement à l'hypothèse ; on peut donc conclure :

$$J = \{0\} \quad \text{ou} \quad \forall x \in A \qquad x = ex$$

e est donc un élément neutre bilatère de A.

Soit alors un élément $b \neq 0$ de A et considérons l'idéal à gauche Ab ; on ne peut avoir $Ab = \{0\}$ car $Ab \ni eb = b \neq 0$; il en résulte que $Ab = A$, ce qui revient à dire que :

$$\forall x \in A \qquad \exists y \qquad yb = x$$

en particulier il existe b' tel que $b'b = e$.

Tout élément non nul de A a donc un inverse à gauche.

$A - \{0\}$ est donc un groupe multiplicatif car il satisfait aux axiomes faibles de la structure de groupe (II, 2, 1) et A est un corps.

Exercice 50.

Soient deux éléments a et b de :

$$\bigcup \{ K ; K \in \mathcal{K} \}$$

Ils sont tels que :

$$\exists K_1 \in \mathcal{K} \qquad a \in K_1 \qquad\qquad \exists K_2 \in \mathcal{K} \qquad b \in K_2$$

mais alors l'hypothèse entraîne que :

$$\exists K \in \mathcal{K} \qquad a \in K \qquad b \in K$$

K étant un sous-corps de E, $a + b$, $a - b$, ab, ab^{-1} (si $b \neq 0$) appartiennent à ce sous-corps, donc à la réunion envisagée et cette réunion est un corps.

Exercice 51.

Soit un polynôme irréductible à coefficients dans un corps K :

$$p = \Sigma\, a_n x^n$$

n décrivant un sous-ensemble fini F de **N** ; et faisons l'extension algébrique de K par rapport à p. Soit θ la racine de p ainsi adjointe :

$$\Sigma\, a_n \theta^n = 0.$$

Dans K(θ), p se factorise. Pour chercher sa factorisation, écrivons :
$x^n = (x - \theta)\,(x^{n-1} + \theta x^{n-2} + \ldots + \theta^{n-2}x + \theta^{n-1}) + \theta^n$.

Appelons q_n le polynôme entre parenthèses, lequel contient n termes, et formons $\Sigma\, a_n x^n$. Il vient :

$$\begin{aligned}\Sigma\, a_n x^n &= (x - \theta)\,\Sigma\, q_n + \Sigma\, a_n \theta^n \\ &= (x - \theta)\Sigma\, q_n.\end{aligned}$$

Donc pour que θ soit racine multiple de p, il faut et il suffit que θ soit racine de l'équation :

$$\Sigma\, q_n = 0.$$

Si K est un corps de caractéristique c et si toutes les valeurs de n sont multiples de c :

$$\forall n \in F \qquad q_n(\theta) = n\theta^{-1} = 0$$

donc :
$$\Sigma\, q_n(\theta) = 0.$$

Réciproquement si $\Sigma\, q_n(\theta) = 0$ c'est que $\Sigma\, n a_n \theta^{n-1} = 0$,
ce qui revient à dire que θ est racine du polynôme :

$$p' = \Sigma\, n a_n x^{n-1}$$

$p'(\theta)$ vaut donc 0 et p' devrait appartenir à l'idéal (p).

Or ce polynôme p' (qui n'est autre, d'ailleurs, que la dérivée de p définie ici algébriquement) est de degré inférieur à celui de p ; il ne peut donc appartenir à l'idéal (p) que s'il est l'élément nul de K$[x]$; ceci exige que :

$$\forall n \in F \quad n a_n = 0 \qquad (1)$$

or a_n ne peut être nul pour tout n car alors p serait identiquement nul ; (1) exige donc que le corps K soit de caractéristique différente de zéro et que tous les n soient des multiples de cette caractéristique.

Remarque : Nous pouvons préciser le degré de multiplicité des racines de l'équation, et montrer qu'il est au moins égal à c. Soit en effet :

$$p = \Sigma\, a_n x^n = \Sigma\, a_n x^{kc}$$

nous avons :
$$0 = \Sigma\, a_n \theta^{kc}$$

et en retranchant membre à membre :

$$p = \Sigma\, a_n\,(x^{kc} - \theta^{kc}) = \Sigma\, a_n\,[(x^c)^k - (\theta^c)^k].$$

Chacune des parenthèses est divisible par $x^c - \theta^c$ qui, dans un corps de caractéristique c, vaut $(x - \theta)^c$.

Exercice 52.

Z_2 ne contient que deux éléments $\dot{0}$ et $\dot{1}$. Pour qu'un polynôme à coefficients dans Z_2 soit irréductible dans ce corps, il faut déjà qu'il ne soit nul ni pour $\dot{0}$ ni pour $\dot{1}$, ce polynôme étant ordonné suivant les puissances croissantes de l'indéterminée il faut donc : 1° que son premier coefficient soit $\dot{1}$; 2° que la somme de ses coefficients soit $\dot{1}$, donc que les coefficients autres que le premier soient en nombre pair.

Ces conditions sont suffisantes pour l'irréductibilité d'un polynôme du deuxième ou du troisième degré dont la factorisation comprendrait nécessairement un polynôme du premier degré. En appliquant les deux règles énoncées ci-dessus, nous trouvons donc tous les polynômes irréductibles du deuxième et du troisième degré :

$(\dot{1}, \dot{1}, \dot{1})$	ou	$1 + x + x^2$
$(\dot{1}, \dot{1}, \dot{0}, \dot{1})$		$1 + x + x^3$
$(\dot{1}, \dot{0}, \dot{1}, \dot{1})$		$1 + x^2 + x^3$.

Les mêmes règles appliquées aux polynômes du quatrième degré donnent les polynômes :

$$(\dot{1}, \dot{1}, \dot{1}, \dot{1}, \dot{1}) \quad (\dot{1}, \dot{1}, \dot{0}, \dot{0}, \dot{1}) \qquad (\dot{1}, \dot{0}, \dot{1}, \dot{0}, \dot{1}) \quad (\dot{1}, \dot{0}, \dot{0}, \dot{1}, \dot{1}).$$

Mais il faut en outre que le polynôme ne soit pas le produit de deux polynômes irréductibles du deuxième degré. Puisque, dans Z_2, nous n'avons trouvé qu'un polynôme irréductible du deuxième degré, son carré est le seul polynôme du quatrième degré à retrancher de la liste précédente, ce carré est le polynôme $(\dot{1}, \dot{0}, \dot{1}, \dot{0}, \dot{1})$ et il reste trois polynômes irréductibles du quatrième degré :

$$\begin{aligned}&1 + x + x^2 + x^3 + x^4 \\ &1 + x + x^4 \\ &1 + x^3 + x^4.\end{aligned}$$

Extensions par rapport à ces polynômes. Pour le premier de ces six polynômes, les éléments de l'extension K(θ) sont des polynômes en θ de degré inférieur à deux et sont donc au nombre de quatre.

Ce sont : $\dot{0} \quad \dot{1} \quad \theta \quad \dot{1} + \theta$,

avec : $\dot{1} + \theta + \theta^2 = 0$,

ce qui donne : $\theta^2 = \dot{1} + \theta$,
car tout élément de Z_2 est égal à son opposé.

On peut former les tables d'opération dans K(θ) :

Addition

	$\dot{0}$	$\dot{1}$	θ	$\dot{1} + \theta$
$\dot{0}$	$\dot{0}$	$\dot{1}$	θ	$\dot{1} + \theta$
$\dot{1}$		$\dot{0}$	$\dot{1} + \theta$	θ
θ			$\dot{0}$	$\dot{1}$
$\dot{1} + \theta$				$\dot{0}$

Multiplication

	$\dot{0}$	$\dot{1}$	θ	$\dot{1} + \theta$
$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$	$\dot{0}$
$\dot{1}$		$\dot{1}$	θ	$\dot{1} + \theta$
θ			$\dot{1} + \theta$	$\dot{1}$
$\dot{1} + \theta$				0

Pour les deux polynômes du troisième degré les corps K(θ) correspondants ont 2^3 éléments (chacun des coefficients d'un polynôme du deuxième degré au plus pouvant prendre la valeur 0 ou la valeur 1) et,

pour les polynômes du quatrième, K(θ) aurait 2^4 éléments. Les tables d'opération s'établiraient comme les précédentes en tenant compte, chaque fois, de la relation vérifiée par θ.

Pour chacun de ces polynômes on pourra chercher sa factorisation dans le corps K(θ) correspondant.

Soit par exemple : $p = \dot{1} + x + x^4$.

Ecrivons : $0 = \dot{1} + \theta + \theta^4$.

Nous trouvons par soustraction :

$$p = (x - \theta) + x^4 - \theta^4 = (x - \theta)(x^3 + \theta x^2 + \theta^2 x + \theta^3 + 1)$$
$$= (x - \theta)(x - \theta - \dot{1})(x^2 + x + \theta^2 + \theta + 1)$$
$$= (x - \theta)(x - \theta - \dot{1})(x - \theta^2)(x - \theta^2 - \dot{1}),$$

K(θ) est donc le corps de factorisation totale du polynôme p.

Remarque : Cette factorisation peut aussi s'écrire :

$$p = (x - \theta)(x - \theta^2)(x - \theta^4)(x - \theta^8) \qquad (1)$$

car : $\theta^4 = 1 + \theta \qquad \theta^8 = 1 + \theta^2$.

Cette dernière forme pouvait être prévue *à priori* (et pourra l'être de façon analogue pour tous nos autres polynômes irréductibles). En effet :

$$p(\theta^{2^k}) = 1 + \theta^{2^k} + (\theta^{2^k})^4 = 1 + \theta^{2^k} + (\theta^4)^{2^k},$$

mais, dans un corps de caractéristique 2, le carré d'une somme est égal à la somme des carrés et :

$$p(\theta^{2^k}) = (1 + \theta^2 + \theta^4)^{2^k} = 0.$$

Tous les θ^{2^k} sont donc racines du polynôme p. Seuls sont distincts θ, θ^2, θ^4, θ^8 car $\theta^{16} = \theta$. D'où la forme (1).

Exercice 53.

Posons $Z = \dfrac{z^3}{z+1}$ (1)

Nous pouvons écrire : $z^3 - zZ - Z = 0$ (2)

ce qui montre que z est une racine du polynôme à une indéterminée :

$p(Z) = x^3 - Zx - Z$ ou $(-Z, -Z, 0, 1)$

à coefficients dans K(Z). K(z) est donc une extension algébrique de K(Z) et si ce polynôme est irréductible dans K(Z) c'est par rapport à lui qu'est faite l'extension. (S'il ne l'était pas z serait racine d'un des polynômes facteurs de p, qui, lui, serait irréductible).

Or, si ce polynôme du troisième degré n'était pas irréductible dans K(Z) c'est qu'il posséderait une racine ; autrement dit il existerait une fraction rationnelle $\dfrac{P}{Q}$ (où P et Q désignent des polynômes en Z) qui vérifierait l'égalité (2), c'est-à-dire aussi l'égalité (1). On devrait donc avoir :

$$\frac{\dfrac{P^3}{Q^3}}{\dfrac{P}{Q} + 1} = \frac{P^3}{Q^2(P+Q)} = Z.$$

Une telle égalité est manifestement impossible car nous pouvons toujours supposer $\dfrac{P}{Q}$ irréductible. Q^2 et $P + Q$ sont alors premiers avec P, donc avec P^3. Et l'égalité ne serait alors possible qu'avec $Q^2(P + Q)$ égal à une constante, mais alors P et Q seraient des constantes et leur quotient ne serait pas Z.

Exercice 54.

Montrer d'un anneau A inclus dans un corps E qu'il est lui-même un corps se réduit à montrer que l'inverse de tout élément de A (qui existe dans E) appartient à A.

Ceci dit, supposons E algébrique sur K et soit $a \in A$; considérons l'extension K(a) qui, puisque a est algébrique, est formée des polynômes K[a]. Ces polynômes en a, à coefficients dans K, font tous partie de A (qui contient K et a). Puisque K[a] est un corps :

$$a^{-1} \in K[a] \subset A.$$

Réciproquement, supposons que tout anneau A tel que $K \subset A \subset E$ soit un corps et soit $a \in E$ un élément quelconque de E.

Nous pouvons considérer l'anneau K[a] formé des polynômes en a à coefficients dans K. D'après l'hypothèse, cet anneau est un corps, mais alors c'est le plus petit corps contenant a et K ; c'est donc K(a) et a est algébrique sur K.

Remarque : On peut se demander par rapport à quel polynôme p est faite l'extension. Soit : $\varphi(a) \in K(a)$ l'élément inverse de a :

$$a\varphi(a) - 1 = 0.$$

Les polynômes φ de K[x] tels que $\varphi(a) = \dfrac{1}{a}$ constituent une classe modulo le polynôme p. Si on nomme φ_0 celui qui a le plus petit degré, le polynôme $x\varphi_0 - 1$ est celui des polynômes qui s'annulent pour $x = a$ qui a le plus petit degré. C'est le polynôme cherché.

Exercice 55.

K(A) est le corps des fractions rationnelles $\dfrac{P}{Q}$ où P et Q sont des polynômes par rapport aux éléments de A et à coefficients dans K :

$$\forall \theta \in A \qquad K(A) \supset K(\theta).$$

Montrons d'abord que tout élément de K(θ) est algébrique sur K. Nous avons vu que les éléments de K(θ) forment un espace vectoriel de dimension n sur K si n est le degré de l'extension.

Soit alors $\beta \in K(\theta)$; les éléments 1, β, β^2 .... β^n sont $n + 1$ éléments de cet espace vectoriel. Nous verrons (au chapitre des espaces vectoriels) que $n + 1$ éléments d'un espace de dimension n sont toujours linéairement dépendants, c'est-à-dire :

$$\exists\, a_0 \ldots\ldots a_n \in K \qquad a_0 + a_1\beta \ldots + a_n\beta^n = 0,$$

autrement dit β est racine d'un polynôme à coefficients dans K. β est algébrique par rapport à K. *Tout élément d'une extension algébrique simple est algébrique.*

De ceci, nous pouvons déduire qu'un élément algébrique quelconque par rapport à K a des puissances, un opposé, un inverse qui sont aussi algébriques.

Montrer que K(A) est algébrique sur K revient alors à montrer que α et β étant deux éléments algébriques sur K, $\alpha + \beta$ et $\alpha\beta$ sont aussi algébriques sur K ; car, s'il en est ainsi, tous les éléments de K(A) étant obtenus par une succession d'opérations donnant des éléments algébriques à partir d'éléments algébriques seront eux-mêmes des éléments algébriques.

Soit donc α et β deux éléments de E tels que K(α) et K(β) soient des extensions algébriques. Cherchons à construire K (α, β) en prenant

$K(\alpha)(\beta)$. α étant algébrique, $K(\alpha)$ est formé de polynômes en α à coefficients dans K. β étant aussi algébrique est racine d'un polynôme irréductible.

$$p \in K[x],$$

mais l'anneau $K[x]$ est inclus dans l'anneau $K(\alpha)[x]$; on peut dire que β est racine d'un polynôme.

$$p \in K(\alpha)[x].$$

(Ce polynôme, irréductible dans K, peut ne pas l'être dans $K(\alpha)$, mais alors β sera racine d'un facteur irréductible dans $K(\alpha)$). L'extension $K(\alpha)(\beta)$ est donc algébrique. Or, $\alpha + \beta$ et $\alpha\beta$ appartiennent à ce corps.

Exercice 56.

1° *La condition est nécessaire.* En effet, si F est algébrique sur K, d'abord, puisque $E \subset F$, les éléments de E sont algébriques sur K ; ensuite, c'est que tout élément θ de F est racine d'un polynôme :

$$p_K \in K[x] \subset E[x]$$

et θ, racine d'un polynôme à coefficients dans E, est algébrique sur E ; donc F est algébrique sur E.

Le polynôme p_K irréductible dans K peut n'être pas irréductible dans E, mais alors θ racine de ce polynôme est racine d'un polynôme p_K *irréductible dans* E *diviseur de* p_K.

2° *La condition est suffisante.* Supposons E algébrique sur K et F algébrique sur E. Tout élément θ de F est racine d'un polynôme irréductible :

$$p_E \in E[x].$$

Les coefficients de ce polynôme forment un sous-ensemble A fini de E. K(A) est un sous-corps de E, algébrique sur K ; et θ appartient à l'extension $K(A)(\theta)$. Or, K(A) s'obtient par l'adjonction successive des différents coefficients de p_K ; chacune de ces extensions étant algébrique, elle se présente comme un espace vectoriel de dimension finie sur la précédente (v. cours III, 5, 3) ; K(A) est donc aussi un espace vectoriel de dimension finie sur K et $K(A)(\theta)$ aussi puisque θ est racine d'un polynôme irréductible à coefficients dans K(A). θ appartient donc à un espace vectoriel de dimension finie n sur le corps K. Les $n + 1$ éléments :

$$1, \theta, \theta^2, \ldots, \theta^n$$

ne peuvent donc pas être indépendants. C'est dire :

$$\exists a_0 \ldots a_i \ldots a_n \in K \qquad \sum_{i=0}^{n} a_i \theta^i = 0.$$

Autrement dit θ est racine d'un polynôme appartenant à $K[x]$ et F est algébrique sur K.

Exemple : Prenons pour K le corps **Q** des rationnels. Prenons pour E l'extension :

$$\mathbf{Q}(\sqrt{2}, \sqrt{3}).$$

On vérifie aisément que ce corps est l'ensemble :

$$E = \{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},\ a, b, c, d \in \mathbf{Q} \},$$

qui forme sur **Q** un espace vectoriel de dimension 4. Soit θ une racine d'un polynôme :

$$p_E = \alpha x^3 + \beta x^2 + \gamma x + \delta \qquad \alpha, \beta, \gamma, \delta \in E.$$

Posons :

$$F = E(\theta).$$

θ est, d'après le raisonnement précédent, algébrique sur **Q** et racine d'un polynôme dont p_E est un diviseur. Vérifions-le directement.

En remplaçant α, β, γ, δ par leurs valeurs et en ordonnant par rapport aux irrationnels, nous trouvons que p_E peut s'écrire :

$$p_E = p\sqrt{2} + q\sqrt{3} + r\sqrt{6} + s,$$

p, q, r, s étant des polynômes du troisième degré à coefficients dans **Q**. Or,

$$(p\sqrt{2} + q\sqrt{3} + r\sqrt{6} + s)(p\sqrt{2} + q\sqrt{3} - r\sqrt{6} - s)$$
$$= 2p^2 + 3q^2 - 6r^2 - s^2 + 2\sqrt{6}(pq - rs)$$

et

$$[2p^2 + 3q^2 - 6r^2 - s^2 + 2\sqrt{6}(pq - rs)]\ [2p^2 + 3q^2 - 6r^2 - s^2 - 2\sqrt{6}(pq - rs)]$$
$$= (2p^2 + 3q^2 - 6r^2 - s^2)^2 - 24(pq - rs)^2.$$

Ce polynôme du douzième degré à coefficients dans **Q** est le polynôme $/_{\mathbf{Q}}$ multiple de p_E dont θ est racine.

Exercice 57.

Un corps fini ne peut avoir une caractéristique nulle puisque ceci entraînerait que l'ensemble $\{ ne\ ;\ n \in \mathbf{Z} \}$ soit infini. Il a donc une caractéristique finie. Par définition de la caractéristique d'un corps (III, 5, 1), ce corps est donc un sur-corps du corps des entiers modulo c ; et ce sur-corps peut être obtenu en faisant un nombre fini d'extensions simples successives. Chacune de ces extensions est algébrique car une extension transcendante aurait un nombre infini d'éléments (le degré des polynômes numérateur et dénominateur n'étant pas limité).

Or, l'extension algébrique $K(\theta)$ de degré n d'un corps K qui a N éléments est formée de polynômes ayant n coefficients à choisir parmi les N éléments de K ; elle a donc N^n éléments.

La première extension simple de Z_c aura donc c^n éléments celle du corps ainsi construit aura $(c^n)^{n'} = c^{nn'}$ éléments et ainsi de suite... le corps fini K obtenu après un nombre fini d'extensions aura un nombre q d'éléments qui sera encore une puissance de c.

$K - \{ 0 \}$ forme pour la multiplication un groupe d'ordre $q - 1$, donc (voir cours page 43) :

$$\forall\ a \in K - \{ 0 \} \qquad a^{q-1} = 1.$$

Il en résulte que $\forall\ a \in K - \{ 0 \}$, a est racine de $x^{q-1} - 1 = 0$, et $\forall\ a \in K$, a est racine de $x^q - x = 0$, qui a ainsi pour racines les q éléments de K.

K est donc le corps de factorisation de ce polynôme.

Posons : $q - 1 = N$ $\qquad$ $K - \{ 0 \} = K'$.

Montrer que K' forme un groupe multiplicatif cyclique revient à montrer qu'il existe au moins une racine α de $x^N - 1 = 0$ telle que :

$$\alpha^N = 1 \quad \text{et} \quad \alpha^n \neq 1 \qquad \forall n < N,$$

ce que nous exprimerons en disant que α est une racine d'ordre N. Remarquons d'abord que pour tout diviseur p de N (premier ou pas) il existe p éléments de K' tels que $x^p = 1$. (Le polynôme $x^p - 1$ admet en effet p racines qui sont toutes racines de $x^N - 1$; car l'identité $x^N - 1 = (x^p - 1)(x^{N-p} + x^{N-2p} + \ldots + x^p + 1)$ est valable dans tout anneau de polynômes à coefficients dans un corps quelconque ou même à coefficients dans un anneau unitaire), ces p éléments forment un sous-groupe de K'.

Remarquons en outre que si p et p' sont premiers entre eux, les deux sous-groupes constitués par les racines de $x^p = 1$ et de $x^{p'} = 1$ ont leur intersection réduite à $\{ 1 \}$ car s'il existait α tel que $\alpha^p = 1$ $\alpha^{p'} = 1$ on

aurait pour λ et μ entiers $\alpha^{\lambda p+\mu p'} = 1$ et on pourrait choisir λ et μ de telle sorte que $\lambda p + \mu p' = 1$, ce qui entraînerait $\alpha = 1$.

Ceci posé, supposons que :

$$N = p^{\lambda}\, p'^{\lambda'}\, p''^{\lambda''} \ldots,$$

p, p', p'' étant des facteurs premiers.

Considérons le sous-groupe de K′ formé des éléments tels que :

$$x^{p^{\lambda}} = 1.$$

Parmi ces éléments, il y en a qui sont d'ordre p^{λ}. En effet, s'ils ne le sont pas ils sont d'ordre p^{μ} avec $\mu < \lambda$ et vérifient donc $x^{p^{\lambda-1}} = 1$. Or, cette équation ne peut avoir p^{λ} racines distinctes.

Soit donc α une racine d'ordre p^{λ} et α' une racine d'ordre $p'^{\lambda'}$ et considérons le produit $\alpha\beta$ et cherchons son ordre. Pour avoir $(\alpha\beta)^m = 1$, il faut avoir $\alpha^m = 1$ et $\beta^m = 1$ car α^m et β^m appartenant à deux sous-groupes dont l'intersection est $\{1\}$ ne peuvent être inverses l'un de l'autre s'ils ne sont pas égaux à 1. Or,

$$\alpha^m = 1,\ \beta^m = 1 \Rightarrow p^{\lambda} | m,\ p'^{\lambda'} | m,$$

$\alpha\beta$ est donc une racine d'ordre $p^{\lambda} p'^{\lambda'}$.

Soit alors γ une racine d'ordre $p''^{\lambda''}$ et considérons le produit $\alpha\beta\gamma$. Le même raisonnement nous montrera que $\alpha\beta\gamma$ est d'ordre $p^{\lambda'} p'^{\lambda'} p''^{\lambda''}$. De proche en proche nous trouverons ainsi une racine d'ordre N.

Exercice 58.

L'ensemble E de toutes les sections commençantes (ouvertes ou fermées) est totalement ordonné par inclusion.

La réunion d'une famille de sections commençantes est une section commençante. A partir de là, il n'y a rien à changer à la démonstration de IV, 2, 2 et l'ensemble E est encore un treillis complet. Tout rationnel définit deux éléments de E (sa section commençante ouverte et sa section commençante fermée). Ces deux éléments de E sont consécutifs, c'est-à-dire qu'entre eux il n'existe aucun élément de E. E contient deux ensembles isomorphes à Q.

Interprétation : Si nous cherchons un ensemble ayant cette structure, nous sommes amenés à penser à celui des suites décimales illimitées, ensemble totalement ordonné lexicographiquement (c'est-à-dire que les chiffres étant numérotés vers la droite à partir de la virgule une suite est antérieure à une autre si leurs chiffres étant égaux jusqu'à l'ordre n, le n^e chiffre de la première est inférieur au n^e chiffre de la deuxième) ; dans cet ensemble il y a bien certains groupes de deux éléments (tels 2, 3499 ... 9 ... et 2, 3500 ... 0 ...) qui représentent un même nombre de **Q**, mais seuls les nombres décimaux ont cette double représentation et non pas tous les rationnels. L'ensemble S des suites ne paraît donc pas fournir l'interprétation que nous cherchons.

Nous allons montrer qu'il est cependant isomorphe pour l'ordre à E à condition d'établir un mode de correspondance correctement choisi entre les éléments des deux ensembles (et non pas en faisant correspondre à chaque suite périodique le rationnel qui en est la limite).

Nous allons commencer par montrer qu'on peut établir un isomorphisme (pour l'ordre) entre **Q** et **D** ensemble des décimaux. **D** et **Q** sont des ensembles dénombrables, ce qui signifie qu'on a pu attribuer un

rang $n \in \mathbf{N}$ à chaque élément $u \in \mathbf{Q}$ et $v \in \mathbf{D}$. Nous faisons d'abord correspondre le premier élément u_0 de **Q** et le premier élément v_0 de **D** :

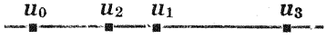
$$u_0 \overset{i}{\longleftrightarrow} v_0,$$

puis on met en correspondance parmi les éléments supérieurs respectivement à u_0 et v_0 les deux éléments u_1 et v_1 qui ont le plus petit rang dans chaque ensemble :

$$u_1 \overset{i}{\longleftrightarrow} v_1$$

Puis on met en correspondance d'une part les éléments de plus petit rang des intervalles $]u_0, u_1[$ et $]v_0, v_1[$, soient $u_2 \overset{i}{\longleftrightarrow} v_2$ et d'autre part les éléments de plus petit rang des intervalles $]u_1, +\infty[$ et $]v_1, +\infty[$, soient $u_3 \overset{i}{\longleftrightarrow} v_3$. Puis on recommence pour les éléments de plus petit rang des intervalles.

$]u_0, u_2[$ et $]v_0, v_2[$
$]u_2, u_1[$ et $]v_2, v_1[$
$]u_1, u_3[$ et $]v_1, v_3[$
$]u_3, +\infty[$ et $]v_3 + \infty[$



et ainsi de suite.....

Chaque intervalle est coupé en deux en mettant chaque fois en correspondance les éléments de plus petit rang de cet intervalle. On procedera de la même façon de l'autre côté de u_0 et v_0.

On peut montrer que tout nombre (de **Q** ou de **D**), quel que soit son rang, finira par être atteint par ce procédé donc par avoir son homologue défini. Soit en effet un nombre $q \in \mathbf{Q}$ de rang p (rien ne serait changé au raisonnement s'il appartenait à **D**). Considérons les bornes de l'intervalle dans lequel il se trouve après chaque dichotomie ; ce sont des nombres de rang inférieur à p (sans quoi c'est q qui aurait été choisi) et à chaque dichotomie une des deux bornes est remplacée par un nombre de rang supérieur. L'ensemble des $2n$ bornes entourant q après n dichotomies forme donc un ensemble de n nombres distincts dont tous les rangs sont inférieurs à p. C'est dire qu'il est forcé que q ait été atteint au plus tard à la p^e dichotomie. La bijection est donc définie pour tout élément de **Q** (ou de **D**). Et il est clair d'après le procédé de construction qu'elle respecte l'ordre (*).

Ceci dit, les sections commençantes ouvertes (resp. fermées) de **Q** sont isomorphes aux sections commençantes ouvertes (resp. fermées) de **D**.

Mais la donnée d'une section commençante de **D** n'est autre que la donnée d'une suite décimale illimitée. [En effet, la donnée d'une telle suite définit une section commençante et, réciproquement, si on connaît une section commençante, on connaît, pour tout n, le plus grand décimal ayant n chiffres après la virgule qui lui appartient, ce qui revient à définir une suite illimitée].

L'isomorphisme i s'étend donc à S, ensemble des suites décimales illimitées et à E, qui sont respectivement les ensembles de toutes les sections commençantes de D et **Q** :

$$S \overset{i}{\longleftrightarrow} E$$

(*) Cette démonstration s'appliquerait à n'importe quel couple d'ensembles *dénombrables totalement ordonnés* et *denses pour l'ordre* dont on a ainsi montré qu'ils peuvent être mis en correspondance biunivoque respectant l'ordre.

Une suite (périodique ou non) dont tous les termes à partir d'un certain rang ne sont pas des 9 ou des zéros correspond à une section commençante ouverte. Le réel (rationnel ou non) qu'elle définit a toujours pour image un réel, non rationnel. Une suite terminée par des 9 et la suite consécutive terminée par des zéros correspondent respectivement à la section commençante ouverte et à la section commençante fermée définissant le même rationnel, image dans i du décimal qui leur est égal.

Exercice 59.

Pour qu'un ensemble T contenant **Q** soit un treillis complet il faut que :

$$\forall X \subset \mathbf{Q} \qquad \sup X \in T$$

Soit donc un ensemble T contenant les bornes supérieures de tous les sous-ensembles de **Q**.

Etant donné un élément a de T considérons l'ensemble :

$$\{ x \in \mathbf{Q} \; ; \; x \prec a \}$$

le signe $\prec$ étant celui de la relation d'ordre sur T, laquelle induit l'ordre ordinaire sur **Q**. Cet ensemble est une section commençante de **Q**, donc un élément de $\overline{\mathbf{R}}$ que nous nommerons $s(a)$. Nous avons donc défini une application f de T dans $\overline{\mathbf{R}}$:

$$\begin{array}{ccc} T & \xrightarrow{f} & \overline{\mathbf{R}} \\ a & & s(a) \end{array}$$

Mais réciproquement une section commençante s de **Q** est un sous-ensemble de **Q** ; son sup est donc un élément b de T et $s(b)$ n'est autre que s. L'application f est donc surjective.

Or, cette application est croissante (c'est-à-dire est un homomorphisme pour l'ordre) car :

$$a \prec b \Rightarrow s(a) \subset s(b)$$

$\overline{\mathbf{R}}$, image homomorphe de T, est donc isomorphe à un ensemble quotient de T. En ne prenant qu'un élément de T par classe d'équivalence nous obtenons un sous-ensemble de T auquel $\overline{\mathbf{R}}$ est isomorphe. Tout treillis complet contenant **Q** contient donc un ensemble isomorphe à $\overline{\mathbf{R}}$ et $\overline{\mathbf{R}}$ est bien, à un isomorphisme près, le plus petit treillis complet contenant **Q**.

Exercice 60.

1° Soit G un groupe totalement ordonné archimédien.

Nous allons essayer de définir une application :

$$\begin{array}{ccc} G & \xrightarrow{f} & \mathbf{R} \end{array}$$

en cherchant à ce qu'elle soit un homomorphisme injectif, c'est-à-dire un isomorphisme de G sur un sous-groupe de **R**.

Soit d'abord a un élément de G. Nous lui ferons correspondre un élément arbitraire de **R**, 1 par exemple.

$$f(a) = 1.$$

Si f doit être un isomorphisme on devra avoir :

$$\forall n \in \mathbf{Z} \qquad f(na) = n.$$

Si G est le groupe monogène infini (*) engendré par a, G sera alors isomorphe au groupe additif **Z**, et la propriété est démontrée.

(*) Dans un groupe ordonné, un sous-groupe ne peut être cyclique.

Si G ne se réduit pas au groupe engendré par a, voyons comment on peut définir $\beta = f(b)$ pour $b \in G \qquad b \notin \{ na \}$.

Puisque G est archimédien tout nombre de la forme mb se place entre deux nombres consécutifs de la forme na :

$$\forall m \in \mathbf{Z} \qquad \exists n_0 \qquad n_0 a \prec mb \prec (n_0 + 1)a$$

et, si f est un isomorphisme pour l'ordre, ceci entraîne :

$$n_0 < m\beta < n_0 + 1.$$

Autrement dit :

$$\forall m \in \mathbf{Z} \qquad \exists n_0 \qquad \frac{n_0}{m} < \beta < \frac{n_0 + 1}{m} \text{ si } m > 0$$

$$\frac{n_0 + 1}{m} < \beta < \frac{n_0}{m} \text{ si } m < 0$$

Ceci revient à dire que β est placé par rapport à tous les rationnels ; β est donc défini par une coupure dans **Q** [ou, ce qui revient au même, tous les nombres rationnels inférieurs à β forment une section commençante]. β est donc un réel défini de façon nécessaire. L'application f est définie.

D'autre part, la façon dont nous avons construit β montre que f est régulière par rapport à l'ordre. Soient en effet $b \prec c$; on pourra toujours trouver $k \in \mathbf{N}$ tel que $kc - kb \prec a$; à ce moment il existera $l \in \mathbf{Z}$ tel que :

$$kb \prec la \prec kc$$

ce qui entraînera :

$$f(b) < \frac{l}{k} \quad \text{et} \quad \frac{l}{k} < f(c)$$

d'après ce qu'on vient de voir ; donc :

$$f(b) < f(c).$$

Ceci montre en outre que f est injective.

Reste à savoir si f est régulière par rapport à l'opération de groupe. Soient b et c deux éléments de G, β et γ leurs images. Soient s_β et s_γ les sections commençantes définissant β et γ. Soient deux rationnels quelconques (qu'on peut toujours supposer réduits à un même dénominateur positif) appartenant respectivement à ces sections :

$$\frac{n}{m} \in s_\beta \qquad \frac{n'}{m} \in s_\gamma$$

$$\frac{n}{m} \in s_\beta \Rightarrow na < mb \qquad \frac{n'}{m} \in s_\gamma \Rightarrow n'a < mc$$

d'où :

$$(n + n')a < m(b + c)$$

puisque G est un groupe ordonné ; d'où :

$$\frac{n + n'}{m} \in s$$

si on désigne par s la section commençante définissant $f(b + c)$. Donc :

$$s_\beta + s_\gamma \subset s \qquad (1).$$

Mais le même raisonnement appliqué aux sections finissantes s'_β, s'_γ, s', montrerait que :

$$s'_\beta + s'_\gamma \subset s' \qquad (2).$$

Les deux premiers membres et les deux seconds membres de (1) et (2) étant complémentaires on peut en conclure :

$$s = s_\beta + s_\gamma$$

c'est-à-dire :

$$f(b + c) = f(b) + f(c)$$

f est donc bien un homomorphisme injectif et la propriété est démontrée.

2° Soit maintenant G satisfaisant aux conditions précédentes et en outre treillis conditionnellement complet et dense pour l'ordre. D'après le 1° il est isomorphe à un sous-groupe E de **R**. Nous allons montrer que E = **R**. Soit en effet un élément x de **R**. Il y a, dans E, des éléments inférieurs à x puisque E est archimédien. Considérons leur ensemble L ; cet ensemble ne peut avoir sa borne supérieure strictement inférieure à x car E étant dense pour l'ordre, L aurait des éléments entre x et cette borne ; pour la même raison, cette borne ne peut être strictement supérieure à x. Donc il admet x pour borne supérieure et x appartient à E.

Exercice 61.

Posons :

$$f(1) = \lambda.$$

Nous avons immédiatement :

$$\forall n \in \mathbf{Z} \qquad f(n) = n\lambda$$

$$\forall m \in \mathbf{Z} \quad f\left(\frac{1}{m}\right) = \frac{1}{m}\lambda \qquad \text{puisque } mf\left(\frac{1}{m}\right) = f\left(\frac{m}{m}\right) = \lambda$$

$$\forall (n, m) \in \mathbf{Z}^2 \quad f\left(\frac{n}{m}\right) = \frac{n}{m}\lambda.$$

Soit alors x réel non rationnel, s sa section commençante, s' sa section finissante. Puisque f est croissante :

$$\forall q \in s \qquad \forall q' \in s' \qquad (q, q') \in \mathbf{Q}^2$$
$$\lambda q < f(x) < \lambda q' \qquad \text{si } \lambda > 0$$
$$\lambda q' < f(x) < \lambda q \qquad \text{si } \lambda < 0$$

$f(x)$ admet donc λs et $\lambda s'$ comme section commençante et section finissante ; c'est donc λx d'après la définition du produit des deux réels.

$$\forall x \in \mathbf{R} \qquad f(x) = \lambda x$$

Remarque : si f n'était pas croissante nous pourrions affirmer :

$$\forall q \in \mathbf{Q} \qquad f(q) = \lambda q$$

mais nous ne pourrions plus rien affirmer pour les réels non rationnels, c'est-à-dire appartenant à $\complement_{\mathbf{R}} \mathbf{Q}$.

Etant donné un de ces irrationnels, $\sqrt{2}$ pour fixer les idées, nous pourrions poser arbitrairement :

$$f(\sqrt{2}) = \mu.$$

On démontrerait comme plus haut que :

$$f\left(\frac{n}{m}\sqrt{2}\right) = \frac{n}{m}\mu$$

et toute expression de la forme :

$$p + \sqrt{2}q \qquad p, q \in \mathbf{Q}$$

aurait alors pour image :

$$\lambda(p + \mu q).$$

Mais nous ne pourrions rien dire pour les réels qui ne seraient pas de cette forme, c'est-à-dire pour ceux qui n'appartiendraient pas à $\mathbf{Q}[\sqrt{2}]$, **R** constituant sur **Q** un espace vectoriel à une infinité de dimensions nous serions ainsi amenés à introduire une infinité de nombres analogues à μ.

Exercice 62.

Nous utiliserons systématiquement le fait suivant : si X est une partie bornée de **R**, il y a au moins un élément x de X tel que :

$$\sup X - \varepsilon < x \leqslant \sup X$$

et un élément x' de X tel que :

$$\inf X \leqslant x' < \inf X + \varepsilon$$

pour tout ε donné réel strictement positif.

Pour abréger l'écriture convenons de noter :

$$\sup_{m > n} x_m = (\sup)_n \qquad \inf_{m > n} x_m = (\inf)_n.$$

Cas L *fini.*

a) Partons de la première définition. Tous les $(\sup)_n$ sont supérieurs à L. Donc pour tout ε et pour tout n il existe un x_m compris entre L — ε et ce sup. Donc :

$$\forall \varepsilon > 0 \qquad \forall n \qquad \exists m > n \qquad x_m > L - \varepsilon.$$

D'autre part L est l'inf des $(\sup)_n$. Donc :

$$\exists n_0 \qquad (\sup)_{n_0} < L + \varepsilon.$$

ce qui entraîne :

$$\forall n > n_0 \qquad x_n < L + \varepsilon.$$

b) Partons de la 2e définition. Tous les $(\sup)_n$ sont inférieurs ou égaux à L car s'il existait $(\sup)_{n_0} < L$ ce serait dire qu'il n'existe aucun élément x_m pour $m > n_0$ compris entre L et ce sup, ce qui est contraire à la 2e partie de la définition. L est donc un minorant de l'ensemble des sup. D'autre part la première partie de la définition entraîne que :

$$\forall \varepsilon \qquad \exists n_0 \qquad (\sup)_{n_0} < L + \varepsilon.$$

Il en résulte que la borne inférieure de ces sup ne peut être supérieure à L car si elle l'était il n'existerait pas de sup entre L et elle. Donc L est bien la borne inférieure de l'ensemble des sup.

Cas où $\overline{\lim}\, x_n = +\infty$.

a) La première définition veut dire que :

$$\forall a \in \mathbf{R}+ \qquad \exists n_0 \qquad (\sup)_{n_0} > a$$

mais alors :

$$\forall \varepsilon \qquad \exists m > n_0 \qquad x_m > a - \varepsilon$$

a et ε étant arbitraires, la 2e définition est bien obtenue.

b) La 2e définition entraîne immédiatement que :

$$\forall n \qquad (\sup)_n = +\infty$$

c'est-à-dire que l'ensemble des $(\sup)_n$ est constitué par l'unique élément de $\overline{\mathbf{R}}$ qui est $+\infty$ (section commençante = **Q**) ; cet ensemble réduit à un seul élément a évidemment cet élément pour borne inférieure et la 2e définition entraîne encore la première.

Cas où $\overline{\lim}\, x_n = -\infty$.

La première définition veut dire :

$$\forall a \in \mathbf{R}+ \qquad \exists n_0 \qquad (\sup)_{n_0} < -a$$

mais ceci entraîne :

$$\forall m > n_0 \qquad x_m < -a.$$

Réciproquement la 2e définition entraîne :

$$\forall a \in \mathbf{R}+ \qquad \exists n_0 \qquad (\sup)_{n_0} < -a$$

mais ceci implique que :

$$\inf |(\sup)_n| = -\infty.$$

Observons que dans ce cas particulier $\overline{\lim}\, x_n = \lim x_n$, la 2° définition n'étant autre que celle de : $\lim x_n = -\infty$.

Exercice 63.

Si on avait :

$$\underline{\lim}\, x_n > \overline{\lim}\, x_n$$

on devrait avoir entre ces deux nombres une infinité de x_n d'après le 2° de la deuxième définition appliquée à $\underline{\lim}\, x_n$ et on ne pourrait en avoir qu'un nombre fini d'après le 1° appliqué à $\overline{\lim}\, x_n$, il y aurait donc contradiction et :

$$\underline{\lim}\, x_n \leqslant \overline{\lim}\, x_n \qquad (1).$$

Si on a l'égalité :

$$\begin{array}{llll} \forall\, \varepsilon & \exists n_0 & \forall\, n > n_0 & x_n < \mathrm{L} + \varepsilon \\ & \exists n_1 & \forall\, n > n_1 & x_n > \mathrm{L} - \varepsilon. \end{array}$$

Donc :

$$\forall\, n > \sup(n_0, n_1) \qquad \mathrm{L} - \varepsilon < x_n < \mathrm{L} + \varepsilon$$

et L est la limite de la suite $\{ x_n \}$.

Remarque importante : L'inégalité (1) a été démontrée ici en utilisant le fait que **R** était totalement ordonné. En fait cette propriété est encore valable dans un treillis complet qui ne serait plus totalement ordonné. En effet :

$$\forall\, n \qquad (\inf)_n \prec (\sup)_n$$

et d'autre part :

$$n < n' \Rightarrow \begin{cases} (\inf)_n \prec (\inf)_{n'} \\ (\sup)_n \succ (\sup)_{n'}. \end{cases}$$

Il en résulte que n'importe quel sup est majorant de tous les inf et le plus petit majorant de ces inf, soit $\underline{\lim}\, x_n$, est donc antérieur à tous les sup, donc à leur plus grand minorant :

$$\underline{\lim}\, x_n \prec \overline{\lim}\, x_n.$$

Quant à l'égalité entre les deux limites supérieure et inférieure, elle ne nous permet plus d'affirmer l'existence d'une limite au sens habituellement donné à ce mot et qui suppose que l'ensemble où est définie la suite est un espace métrique. Mais comme cela a été signalé dans la remarque IV, 2, 6, c'est un nouveau moyen de définir une limite sans avoir préalablement défini une distance.

Exercice 64.

$s(x_n)$ désigne la section commençante ouverte formée de tous les réels strictement inférieurs à x_n.

$$\overline{\lim}\, s(x_n) = \bigcap_{n \in \mathrm{N}} \bigcup_{m > n} s(x_m).$$

Cherchons d'abord ce que représente $\bigcup_{m>n} s(x_m)$. Cet ensemble est identique à :

$$s(\sup_{m>n} x_m)$$

car si x appartient au premier de ces deux ensembles, il appartient au 2° et s'il appartient au 2°, il existe un rationnel entre lui et $\sup_{m>n} x_m$; ce rationnel appartient à la section commençante ouverte de **Q** définissant $\sup_{m>n} x_m$ qui est la réunion des sections commençantes ouvertes de **Q** définissant les x_m ; donc il appartient à une de ces sections, donc à la section commençante de **R** qui la contient, donc à $\bigcup_{m>n} s(x_m)$.

On peut donc écrire :

$$\bigcup_{m>n} s(x_m) = s(\sup_{m>n} x_m)$$

et :

$$\overline{\lim}\, s(x_n) = \bigcap_{n \in \mathrm{N}} s(\sup_{m>n} x_m).$$

Posons :

$$\sup_{m>n} x_m = y_n$$

et comparons :

$$\bigcap_{n \in \mathrm{N}} s(y_n) \text{ et } s(\inf_{n \in \mathrm{N}} y_n).$$

Tout élément du 2° ensemble appartient évidemment au premier. Tout élément du premier ensemble étant inférieur à tous les y_n appartient à la section commençante ouverte, ou fermée, de $\inf y_n$. [En effet si $\inf y_n \notin \{ y_n \}$, $\inf y_n$ appartient à toutes les sections ouvertes $s(y_n)$ et l'intersection de ces sections ouvertes est fermée ; si, au contraire, $\inf y_n$ est un des y_n, soit y_p, il n'appartient pas à $s(y_p)$, donc pas à l'intersection et celle-ci est une section ouverte]. On peut donc seulement dire :

$$\overline{\lim}\, s(x_n) = s(\overline{\lim}\, x_n) \text{ ou } \overline{\lim}\, s(x_n) = \sigma(\overline{\lim}\, x_n),$$

σ représentant la section commençante fermée définie par $\overline{\lim}\, x_n$.

Exercice 65.

Plongement d'un ensemble ordonné dans un treillis complet.

Question préliminaire. Soient $\mathrm{X} \subset \mathrm{E}$ et $\mathrm{Y} \subset \mathrm{E}$.

Si $\mathrm{X} \subset \mathrm{Y}$, on a : $\forall\, x \in \mathrm{Y} \quad u > x \Rightarrow \forall\, x \in \mathrm{X} \quad u > x$

c'est-à-dire :

$$u \in \mathrm{Y}^+ \Rightarrow u \in \mathrm{X}^+$$

ou :

$$\mathrm{Y}^+ \subset \mathrm{X}^+.$$

On montrerait de même que :

$$\mathrm{Y}^- \subset \mathrm{X}^-$$

et par conséquent :

$$\mathrm{X} \subset \mathrm{Y} \Rightarrow \mathrm{Y}^+ \subset \mathrm{X}^+ \Rightarrow \mathrm{X}^{+-} \subset \mathrm{Y}^{+-}$$

et :

$$\mathrm{X} \subset \mathrm{Y} \Rightarrow \mathrm{Y}^- \subset \mathrm{X}^- \Rightarrow \mathrm{X}^{-+} \subset \mathrm{Y}^{-+}$$

Considérons alors X^{+-}, cet ensemble est constitué de tous les éléments antérieurs à tous les éléments de X^+. Il est donc évident qu'il contient tous les éléments de X :

$$\mathrm{X} \subset \mathrm{X}^{+-} \qquad (1)$$

ce qui, en vertu de la remarque précédente, entraîne :

$$\mathrm{X}^+ \supset \mathrm{X}^{+-+} \qquad (2).$$

Mais d'autre part posons $\mathrm{X}^+ = \mathrm{Y}$ et appliquons à Y l'inclusion évidente comparable à celle (1) utilisée ci-dessus :

$$\mathrm{Y} \subset \mathrm{Y}^{-+}.$$

Il vient :

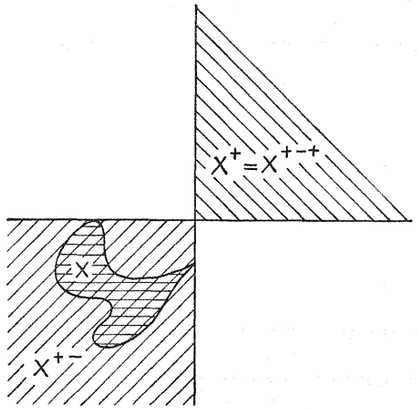
$$X^+ \subset X^{+-+}$$

qui, rapprochée de (2), donne :

$$X^+ = X^{+-+}.$$

On montrerait de même que :

$$X^- = X^{-+-}.$$



I. *a*) $\{ X_i \}$ étant une famille de parties de E, $\bigcap X_i^-$ est l'ensemble des x qui sont antérieurs à tous les éléments de tous les X_i, donc aux éléments de la réunion des X_i.

$$\bigcap X_i^- = \{ u \ ; \quad \forall x \in \bigcup X_i \ , \ u \prec x \} = (\bigcup X_i)^-.$$

Il en résulte que $\bigcap X_i^-$ est un élément de T. C'est un minorant de $\{ X_i^- \}$ et c'est évidemment le plus grand ; donc cet ensemble possède une borne inférieure :

$$\inf \{ X_i^- \} = (\bigcup X_i)^- \qquad (1).$$

b) D'autre part nous avons démontré (IV, 2, 2) un théorème dont le corrélatif est : si un ensemble ordonné possède un plus grand élément et si tout sous-ensemble de cet ensemble admet une borne inférieure, il admet aussi une borne supérieure.

Or l'ensemble T, ordonné par inclusion, possède un plus grand élément si E possède lui-même un plus grand élément ω. Car ω^-, ensemble des minorants de ω, est E lui-même.

Si E ne possède pas de plus grand élément nous pourrons quand même admettre que E fait partie de l'ensemble T. On peut en effet vérifier que la règle précédemment établie et traduite par l'égalité (1) ne sera pas en défaut si on range E parmi les X^- en posant :

$$E = \emptyset^-.$$

Le théorème cité ci-dessus s'applique donc dans tous les cas et T est un treillis complet.

II. Etudions maintenant ce que les structures de T induisent sur l'ensemble E, image de E par la bijection :

$$a \longleftrightarrow a^- = \tilde{a}$$

(a^- est une partie de E, mais c'est un élément de $\tilde{E}$ que nous nommons $\tilde{a}$).

Soient a et b deux éléments de E tels que $a \prec b$.

Ceci entraîne :

$$a^- \subset b^-$$

donc sur $\tilde{E}$:

$$\tilde{a} \prec \tilde{b}.$$

L'ordre sur T induit donc sur $\tilde{E}$ l'ordre image de celui de E dans la bijection.

Voyons maintenant si, dans le cas où un ensemble $X \subset E$ possède un inf et un sup, ce sont bien leurs images par la bijection qui sont inf $\tilde{X}$ et sup $\tilde{X}$, $\tilde{X}$ étant l'image de X. On a d'abord, en appliquant l'égalité (1) :

$$\inf \tilde{X} = \left\{ \bigcup \{ x \} \ ; \ x \in X^- \right\} = X^-.$$

Si X possédait une borne inférieure, inf X :

$$X^- = (\inf X)^-$$

donc :

$$\inf \tilde{X} = (\inf X)^-$$

et, dans la bijection, inf X a pour image inf $\tilde{X}$:

$$\inf \tilde{X} = \widetilde{\inf X}.$$

Passons maintenant à l'étude des sup. Le fait que :

$$\forall a, b \in E \qquad a \prec b \Rightarrow \tilde{a} \prec \tilde{b}$$

entraîne que :

$$a \in X^+ \Rightarrow \tilde{a} \in (\tilde{X})^+$$

ou :

$$\widetilde{X^+} \subset (\tilde{X})^+.$$

Mais alors le plus petit élément de $(\tilde{X})^+$ qui est sup $\tilde{X}$ est antérieur au plus petit élément de $\widetilde{X^+}$; celui-ci est (toujours en vertu de la conservation de l'ordre dans la bijection) l'image du plus petit élément de X^+, c'est-à-dire sup X ; on peut donc écrire :

$$\sup \tilde{X} \prec \widetilde{\sup X}.$$

Mais d'autre part un majorant de $\tilde{X}$ est un ensemble de la forme Y^- qui contient $\tilde{X}$ et pour contenir $\tilde{X}$ il est nécessaire et suffisant qu'il contienne X. Le plus petit de ces majorants est leur intersection. C'est en effet la borne inférieure de leur ensemble et on vient de montrer qu'elle était l'intersection.

On peut donc poser :

$$\sup \tilde{X} = \bigcap \{ Y^- \ ; \ Y^- \supset X \} .$$

On a donc :

$$\forall x \in X \qquad x \in Y^-$$

ce qui entraîne :

$$\forall x \in X \qquad x^+ \supset Y^{-+}.$$

Donc :

$$\bigcap \{ x^+ \ ; \ x \in X \} \supset Y^{-+}.$$

Or :

$$\bigcap \{ x^+ \ ; \ x \in X \} = (\sup X)^+$$

donc :

$$(\sup X)^{+} \supset Y^{-+}$$

ceci s'étendant à tous les Y tels que $Y^{-} \supset X$.

D'après la question préliminaire cette dernière inclusion entraîne :

$$(\sup X)^{+-} \subset Y^{-+-}$$

$(\sup X)^{+-}$ n'est autre que $(\sup X)^{-}$ (il suffit de se reporter à la définition) $Y^{-+-} = Y^{-}$ d'après la question préliminaire. Donc :

$$\forall\, Y^{-} \supset X \qquad (\sup X)^{-} \subset Y^{-}.$$

Donc :

$$(\sup X)^{-} \supset \bigcap \{\, Y^{-} ;\ Y^{-} \supset X \,\},$$

c'est-à-dire :

$$\widetilde{\sup X} \prec \sup \tilde{X}.$$

En rapprochant de l'inégalité opposée on voit qu'on a l'égalité des sup.

Exercice 66.

Complétion d'un espace métrique :

1° *a*) Montrons que $d(x_n, y_n)$ est une suite de Cauchy de **R**, ce qui suffira à établir sa convergence. Evaluons donc :

$$|d(x_n, y_n) - d(x_m, y_m)|.$$

On sait que :

$$d(x_n, y_n) < d(x_n, x_m) + d(x_m, y_m) + d(y_m, y_n),$$

donc :

$$d(x_n, y_n) - d(x_m, y_m) < d(x_n, x_m) + d(y_m, y_n).$$

Et de même :

$$d(x_m, y_m) - d(x_n, y_n) < d(x_n, x_m) + d(y_n, y_m).$$

Donc :

$$|d(x_m, y_m) - d(x_n, y_n)| < d(x_n, x_m) + d(y_n, y_m).$$

Or, puisque $\{ x_n \}$ et $\{ y_n \}$ sont des suites de Cauchy,

$$\forall \varepsilon \in \mathbf{R}^{+} \quad \exists n_0 \quad \forall n, m > n_0 \qquad d(x_n, x_m) < \varepsilon$$
$$\exists n_1 \quad \forall n, m > n_1 \qquad d(y_n, y_m) < \varepsilon.$$

Donc :

$$\forall n, m > \sup(n_0, n_1) \qquad |d(x_n, y_n) - d(x_m, y_m)| < 2\varepsilon.$$

b) Soient x' et y' appartenant respectivement aux classes de x et y, nous devons montrer que :

$$d(x, y) = d(x', y'),$$

c'est-à-dire que :

$$\lim [d(x_n, y_n) - d(x'_n, y'_n)] = 0.$$

Or, de la même façon que ci-dessus, on peut écrire :

$$|d(x_n, y_n) - d(x'_n, y'_n)| < d(x_n, x'_n) + d(y_n, y'_n).$$

Puisque $\{ x_n \}\ \mathrm{R}\ \{ x'_n \}$, $d(x_n, x'_n)$ a pour limite 0,
donc, $\forall \varepsilon \in \mathbf{R}^{+} \quad \exists n_0 \quad \forall n > n_0 \quad d(x_n, x'_n) < \varepsilon$,
et de même : $\exists n_1 \quad \forall n > n_1 \ d(y_n, y'_n) < \varepsilon$,
donc : $\forall n > \sup(n_0, n_1) \qquad |d(x_n, y_n) - d(x'_n, y'_n)| < 2\varepsilon$,
ce qui entraîne bien que la limite de cette quantité soit nulle.

c) L'application définie est bien une distance car :

$$d(x, y) = 0 \iff \lim d(x_n, y_n) = 0 \iff \dot{x} = \dot{y},$$

L'égalité $d(x, y) = d(y, x)$ est évidente ;
enfin $d(x_n, z_n) \leqslant d(x_n, y_n) + d(y_n, z_n)$,
donc : $\lim d(x_n, z_n) \leqslant \lim d(x_n, y_n) + \lim d(y_n, z_n)$.

2° $\dot{\mathrm{E}}$ sera l'ensemble des classes de suites de Cauchy de E qui convergent dans E.

On peut définir la bijection :

$$\dot{\mathrm{E}} \longleftrightarrow \mathrm{E}$$
$$\dot{x} \longleftrightarrow x$$

en faisant correspondre à tout élément x de E la classe $\dot{x}$ des suites de Cauchy qui convergent vers cet élément, classe qui contient en particulier la suite constante $\{ x \}$ dont tous les termes sont égaux à cet élément.

Cette bijection est une isométrie car :

$$d(\dot{x}, \dot{y}) = \lim d(x, y) = d(x, y).$$

3° Il n'y a rien à changer (sauf les notations) aux démonstrations des deux mêmes propriétés lors de la complétion de **Q** en **R** (voir cours IV, 3, 4).

4° Soit F un ensemble répondant aux conditions de l'énoncé, c'est-à-dire qui soit un espace métrique incluant E et sur lequel E soit dense. Etant donné un élément ξ de F, le fait que E soit dense sur F permet d'affirmer qu'il existe des suites de Cauchy de E qui convergent vers ξ. Il suffit, en effet, de se donner une suite de réels $\{ \varepsilon_n \}$ tendant vers zéro $\left(\text{par exemple } \varepsilon_n = \frac{1}{n}\right)$ et de choisir x_n pour que $d(x_n, \xi) < \varepsilon_n$ pour obtenir une suite $\{ x_n \}$ de E convergeant vers ξ.

Mais ceci nous fournit une infinité de suites de Cauchy qui ayant même limite appartiennent à la même classe de $\mathcal{C}$ (mod R). A un élément x de F on fait donc correspondre un élément de $\widehat{\mathrm{E}}$. Mais, réciproquement, un élément de $\widehat{\mathrm{E}}$ est une classe de $\mathcal{C}$ (mod R). Les suites de cette classe convergent vers un élément de F puisque F est complet et que les suites dans E sont des suites dans F ; et elles convergent vers le même élément. Donc à un élément de $\widehat{\mathrm{E}}$ correspond un élément de F et nous avons bien une bijection :

$$\mathrm{F} \longleftrightarrow \widehat{\mathrm{E}}.$$

Reste à montrer que cette bijection est une isométrie. Soient deux éléments ξ et η de F et deux suites de Cauchy $\{ x_n \}$ et $\{ y_n \}$ de E qui convergent respectivement vers ξ et η.

$$d(\xi, \eta) < d(x_n, \xi) + d(y_n, x_n) + d(y_n, \eta)$$

(d désigne ici la distance définie sur F qui induit sur E la distance qui y était initialement définie). Ceci donne :

$$|d(\xi, \eta) - d(y_n, x_n)| < d(x_n, \xi) + d(y_n, \eta).$$

Pour n assez grand, le second membre sera inférieur à ε donné : c'est-à-dire que $d(y_n, x_n)$ converge vers $d(\xi, \eta)$. Or, $\lim d(y_n, x_n)$ était précisément la distance des classes de $\{ x_n \}$ et $\{ y_n \}$ telle qu'on l'avait définie sur $\widehat{\mathrm{E}}$. L'isométrie est donc bien établie.

Index terminologique

Le premier numéro renvoie au chapitre, le second au paragraphe, le troisième au sous-paragraphe.

IMP. A. COUESLANT
CAHORS — 97.962
Dépôt légal : IV-1962

Association des Professeurs de Mathématiques
de l'Enseignement Public,
29, rue d'Ulm, Paris (5°)

EXTRAIT DES STATUTS

Article II. — L'Association a pour but l'étude des questions intéressant l'enseignement des Mathématiques et la défense des intérêts professionnels de ses membres. Elle institue ou encourage des réunions, des discussions, des enquêtes sur l'enseignement des Mathématiques en France ou à l'étranger...

L'A.P.M. est ouverte à tous les Collègues enseignant dans les Facultés, les Grandes Ecoles, les Lycées, classiques, modernes ou techniques, les Ecoles Nationales Professionnelles, les Collèges d'Enseignement Général ou les Collèges Techniques.

COTISATION. — Elle comprend l'abonnement au Bulletin, ainsi que les fascicules d'énoncés.

Cotisation normale ..... 10 NF

Cotisation réduite (stagiaires C.P.R., élèves des E.N.S. et des I.P.E.S., jeunes gens accomplissant leur service militaire, retraités) ..... 5 NF

ABONNEMENT (personnes n'appartenant pas à l'Enseignement Public, bibliothèques, etc...) :

France et Communauté : 12 NF - Autres pays : 15 NF

Le numéro : 3 NF

MODE DE PAIEMENT. — Virement postal (adressé au centre de chèques du tireur) ou mandat-carte à l'adresse :

A.P.M., 29, rue d'Ulm - PARIS, 5° - C.C.P. Paris 5708-21

RECOMMANDATIONS DU TRESORIER. — Indications à porter sur le talon du chèque : 1° Nom (en majuscules) et prénom. — 2° Adresse où doit être envoyé le Bulletin. — 3° Ancienne adresse en cas de changement. — 4° Nom de l'établissement où l'on exerce. — 5° Nom de l'établissement précédent en cas de mutation en fin d'année scolaire.

N. B. — Toute nouvelle adhésion demandée en cours d'année scolaire compte à partir du 1er octobre précédent. Elle donne droit à tous les bulletins déjà parus au cours de l'année scolaire, sous réserve qu'ils ne soient pas épuisés.

Voir, page 2 de la couverture, la liste des brochures de l'A.P.M.