Séminaire Dubreil.
Algèbre et théorie
des nombres

Marc Krasner

Endothéorie de Galois abstraite

Séminaire Dubreil. Algèbre et théorie des nombres, tome 22, n° 1 (1968-1969), exp. n° 6, p. 1-19

<http://www.numdam.org/item?id=SD_1968-1969__22_1_A4_0>

Séminaire DUBREIL-PISOT
Algèbre et Théorie des nombres)
22e année, 1968/69, n° 6, 19 p.

6 et 13 janvier 1969

ENDOTHÉORIE DE GALOIS ABSTRAITE

par Marc KRASNER

Résumé

1. Idée de la théorie et de l'endothéorie de Galois abstraites.

Plaçons-nous dans le cadre de la théorie de Galois classique. On a un corps k, dit corps de base, et une extension de degré fini K de k, qui est normale, c'est-à-dire telle que tout polynôme irréductible (dans k) appartenant à $k[X]$, qui a au moins un zéro dans K, s'y décompose en facteurs linéaires en X. Une application

$$\sigma : K \to K$$

est dite un automorphisme de l'extension K/k, si :

1° Pour tous $x, y \in K$, on a $\sigma.(x + y) = \sigma.x + \sigma.y$ [1] ;

2° Pour tous $x, y \in K$, on a $\sigma.xy = (\sigma.x)(\sigma.y)$;

3° Pour tout $\alpha \in k$, on a $\sigma.\alpha = \alpha$.

Il est à remarquer que les conditions précédentes entraînent que σ est bijective, autrement dit, est une permutation de K, d'où il résulte que leur ensemble $G_{K/k}$ est, par rapport à la composition des autoapplications de K, un groupe de permutations de cet ensemble, dit le groupe de Galois de K/k.

Soit $A \subseteq K$. Considérons le sous-ensemble $G_{K/k,A}$ de $G_{K/k}$ (qui en est un sous-groupe) formé des $\sigma \in G_{K/k}$, qui préservent tout élément a de A, c'est-à-dire satisfont à la condition :

4° Pour tout $a \in A$, on a $\sigma.a = a$.

La théorie de Galois classique (du moins, envisagée d'un certain point de vue) donne les réponses aux deux questions suivantes qu'il est naturel de se poser :

---

[1] Si σ est une application d'un ensemble A, l'image par σ d'un $a \in A$ sera toujours écrite $\sigma.a$ (avec le point . au milieu). Par contre, si A est muni d'une loi de composition (interne), le composé sera écrit, en général, ab, et jamais $a.b$.

Premier problème de Galois : Quel est l'ensemble $\bar{A}$ des $x \in K$, qui sont préservés par tout $\sigma \in G_{K/k,A}$ (autrement dit, par tout automorphisme de K/k préservant tout $a \in A$) ?

Deuxième problème de Galois : Quels sous-groupes g de $G_{K/k}$ sont, pour quelque $A \subseteq K$, de la forme $G_{K/k,A}$ (autrement dit, sont des ensembles complets des automorphismes de K/k préservant tout élément de quelque sous-ensemble de K) ?

Il est bien connu que les réponses à ces problèmes, données par la théorie considérée, sont les suivantes :

(1) L'ensemble $\bar{A}$ est la fermeture de A par rapport aux opérations rationnelles $x + y$, xy (définies partout sur $K \times K$) et x^{-1} (définie pour tout $x \in K$ non nul), et, quand la caractéristique p de k n'est pas nulle, par rapport à l'extraction $\sqrt[p]{x}$ de la racine p-ième de x (définie pour les $x \in K$, qui sont les puissances p-ièmes d'autres éléments de K).

(2) Tout sous-groupe g de $G_{K/k}$ est, pour un $A \subseteq K$ convenable, de la forme $G_{K/k,A}$.

La définition précédente des automorphismes de K/k et de ceux d'entre eux qui appartiennent à $G_{K/k,A}$ semble, à première vue, comporter des conditions de nature hétérogène : d'une part, on exige la préservation de certaines opérations $(x + y , xy)$, d'autre part, celle de certains éléments de K $(\alpha \in k , a \in A)$. Mais, en examinant la situation plus attentivement, on s'aperçoit que, dans tous les cas, ces conditions peuvent se formuler comme imposant (indifféremment) à σ l'une des deux exigences : celle de laisser stables ou celle de préserver certaines relations, dont certaines sont de dimension (ou "arité") 3 et d'autres de dimension 1. Les termes qu'on vient d'employer seront précisés plus loin d'une manière rigoureuse. Disons, pour le moment, d'une manière un peu vague, qu'une autoapplication φ d'un ensemble E laisse stable une relation (de dimension arbitraire) sur cet ensemble, si elle transforme toute configuration d'éléments de E, qui satisfait à cette relation, en une configuration, qui y satisfait encore. Et disons que φ préserve la relation considérée, si, également, elle transforme une configuration ne satisfaisant pas à la relation en une configuration qui n'y satisfait pas.

En effet, les conditions 1°, 2°, équivalent respectivement aux :

1°' Pour tous $x , y , z \in K$, $x + y = z$ implique $\sigma.x + \sigma.y = \sigma.z$;
2°' Pour tous $x , y , z \in K$, $xy = z$ implique $(\sigma.x)(\sigma.y) = \sigma.z$.

Quant à $\sigma.\alpha = \alpha$ $(\alpha \in k)$ ou $\sigma.a = a$ $(a \in A)$, ces égalités équivalent respectivement aux :

3°' Pour tout $x \in K$, $x = \alpha$ implique $\sigma.x = \alpha$;
4°' Pour tout $x \in K$, $x = a$ implique $\sigma.x = a$.

Ainsi, on peut formuler 1°, 2°, 3°, 4° : σ laisse stable les relations respectives : $+(X , Y , Z)$, qui est telle que $(x , y , z) \in +(X , Y , Z)$ si, et seulement si, $x + y = z$; $\times(X , Y , Z)$, qui est telle que $(x , y , z) \in \times(X , Y , Z)$ si, et seulement si, $xy = z$; pour tout $\alpha \in k$, la relation $(\alpha ; X)$, telle que $x \in (\alpha ; X)$ si, et seulement si, $x = \alpha$; pour tout $a \in A$, la relation $(a ; X)$, analogue.

Mais, comme toute autoapplication de K satisfaisant aux 1°, 2°, 3°, est bijective, elle satisfait aussi aux conditions : pour tous $x , y , z \in K$, $x + y \neq z$ implique $\sigma.x + \sigma.y \neq \sigma.z$, et $xy \neq z$ implique $(\sigma.x)(\sigma.y) \neq \sigma.z$; pour tout $\alpha \in k$, $x \neq \alpha$ $(x \in K)$ implique $\sigma.x \neq \alpha$. En plus, si un tel σ satisfait à 4°, on a aussi, quel que soit $a \in A$, pour tout $x \in K$, $x \neq a$ implique $\sigma.x \neq a$. Ainsi, les automorphismes de K/k peuvent se définir aussi comme ses autoapplications (ou permutations) préservant $+(X , Y , Z)$, $\times(X , Y , Z)$, et, pour tout $\alpha \in k$, $(\alpha ; X)$, et la condition 4° peut se formuler pour eux comme préservation, pour tout $a \in A$, de $(a ; X)$.

Dès lors, le premier problème de Galois peut aussi se formuler des deux manières suivantes :

(1) Quel est l'ensemble des relations de la forme $(x ; X)$ que préserve toute permutation σ de K , qui préserve les relations $+(X , Y , Z)$, $\times(X , Y , Z)$, les $(\alpha ; X)$ pour tout $\alpha \in k$, et les $(a ; X)$ pour tout $a \in A$?

(2) Quel est l'ensemble des relations de la forme $(x ; X)$ que laisse stable toute autoapplication φ de K , qui laisse stable toutes les relations énumérées dans (1) ?

Quand on pose le problème sous une de ces formes, l'idée vient d'étendre chacune de ces deux formulations aux ensembles quelconques R de relations (d'arité arbitraire et pas forcément finie) d'un ensemble quelconque E , c'est-à-dire aux structures arbitraires de premier ordre. Etant donnée une telle structure $S = (E , R)$, les analogues des (1) et (2) pour S sont :

(1') Quel est l'ensemble $\overline{R}$ des relations de E , qui sont préservées par toute permutation σ de E , qui préserve toute $r \in R$?

(2') Quel est l'ensemble $\overline{\overline{R}}$ des relations de E , que laisse stable toute autoapplication φ de E , qui laisse stable toute $r \in R$?

Les mots "Quel est l'ensemble, etc." formulent incomplètement les problèmes qu'on se pose, car on aimerait avoir leur solution sous une forme un peu analogue à celle du cas classique. D'une manière plus précise, on aimerait avoir des caractérisations des ensembles $\overline{R}$, $\overline{\overline{R}}$ comme fermetures de R par rapport aux familles convenables d'opérations. Bien entendu, vu la généralité du contexte, il ne peut pas

s'agir d'opérations particulières sur les configurations d'éléments de E (comme, par exemple, l'addition ou la multiplication), mais seulement (si cela est réalisable) d'opérations très générales de nature ensembliste sur les relations arbitraires d'un ensemble arbitraire E . On peut, d'autre part, poser aussi, dans ce contexte, les questions suivantes, analogues au deuxième problème de la théorie de Galois classique :

(1") Quels groupes de permutations de E sont les ensembles de toutes les permutations préservant toute relation appartenant à quelque ensemble convenable de relations de E ?

(2") Quels demi-groupes d'autoapplications de E sont les ensembles de toutes les autoapplications laissant stable toute relation appartenant à quelque ensemble convenable de relations de E ?

J'ai effectivement trouvé une famille d'opérations sur les relations ou configurations de relations d'un ensemble arbitraire E , que j'appelle opérations fondamentales, telle que $\bar{R}$ soit la fermeture de R par rapport aux opérations de cette famille. De même, j'ai pu déterminer une sous-famille de la famille précédente, que j'appelle la famille des opérations fondamentales directes, telle que $\bar{\bar{R}}$ soit la fermeture de R par rapport aux opérations de cette sous-famille. La théorie de Galois abstraite est l'étude de dualité entre les relations d'un ensemble (arbitraire) E et les permutations de E qui les préservent, analogue à la théorie de Galois classique (donc centrée sur les problèmes (1'), (2')), mais où le rôle des opérations rationnelles (et de l'extraction éventuelle de la racine p-ième) sur les éléments du support est joué par les opérations fondamentales sur les relations dans le support. Et, de même, l'endothéorie de Galois abstraite est une théorie de dualité analogue entre les relations de E et les autoapplications de E qui les laissent stables, centrée sur les problèmes (1"), (2"), et où le rôle des opérations des corps, intervenant dans la théorie de Galois classique, est joué par les opérations fondamentales directes.

C'est en 1935 que j'ai eue l'idée de la théorie de Galois abstraite, qui a été publiée, pour la première fois (avec les démonstrations complètes, mais avec une différence inessentielle de présentation) en 1938 [1] sous le titre peu adéquat "Une généralisation de la notion de corps". J'ai publié, à plusieurs reprises, les résumés de la forme définitive de cette théorie ([2], [3], [4], [5]), dont certains ([2], [3]) contiennent aussi les résumés (provisoires) de certains développements ultérieurs (théorie de Galois multiplicitaire, théorie des structures éliminatives) pas encore publiés sous une forme complète (toutefois, ces théories, sous la forme définitive qu'elles ont prise, ont été déjà exposées dans mes cours de la théorie de Galois abstraite donnés à la Faculté des Sciences de Clermont-Ferrand en 1959/60

et en 1963/64, et j'ai commencé de les exposer dans le cours du même nom que je donne actuellement à l'Université Paris-VI). Quant à l'endothéorie de Galois abstraite, j'ai soupçonné dès le début la possibilité d'une théorie basée sur la stabilité par rapport aux autoapplications au lieu de préservation par permutations, mais je n'ai trouvé une telle théorie effectivement qu'en 1965. Le seul résumé actuellement publié (d'ailleurs pas tout-à-fait exact en ce qui concerne la formulation du "théorème d'homomorphisme") est le texte [6] des "Abstracts" (partie "Algebra") du Congrès international des Mathématiciens, Moscou, 1966, résumant la communication que j'y ai faite sur ce sujet. Toutefois, la fin du chapitre VI du polycopié (non édité commercialement) de mon cours "Théorie de Galois classique et abstraite", fait en 1966/67 à la Faculté des Sciences de Paris, est un exposé (avec démonstrations), rédigé par moi-même, de l'endothéorie de Galois abstraite, à part le théorème d'homomorphisme (le début du même chapitre est un exposé de la théorie de Galois abstraite, rédigé par mon ancien assistant I. HAJJ).

2. Opérations fondamentales et opérations fondamentales directes.

Soient E un ensemble dit le support, et X un ensemble dit ensemble des variables (ou des noms des variables). On appellera X-points de E, les applications $P : X \to E$, et on appellera X-relations de (ou dans) E, les ensembles de X-points de E. Ainsi, un X-point de E est un élément arbitraire de E^X, et une X-relation de E est un sous-ensemble arbitraire du même ensemble. S'il n'y a pas de doute possible sur X, sur E, ou sur les deux à la fois, on parlera respectivement de points et relations de E, de X-points et X-relations, ou de points et relations tout court. Avant de définir les opérations fondamentales (qui concernent les points avec l'ensemble des coordonnées fixé et, par ailleurs, arbitraire), on va introduire deux identifications (dites première et seconde identifications canoniques) pour les points (et ensembles de points) ayant leurs ensembles de coordonnées différents, mais liés de certaines manières.

1° Soit $\overline{X} \subseteq X$. Un $\overline{X}$-point $\overline{P} : \overline{X} \to E$ sera identifié, dans la première identification canonique, avec l'ensemble des X-points $P : X \to E$, dont la restriction à $\overline{X}$ soit $\overline{P}$, autrement dit à $\overline{P} \times E^{X..\overline{X}}$. Cette identification sera étendue "par additivité" aux ensembles de points, c'est-à-dire aux $\overline{X}$-relations, une telle relation $\overline{r}$ étant identifiée au produit cartésien $\overline{r} \times E^{X..\overline{X}}$.

Remarque. - On constate que les premières identifications canoniques pour tous les couples $(X , \overline{X} \subseteq X)$, étendues par transitivité, constituent un système cohérent d'identifications, autrement dit conduisent à une équivalence dans la classe des relations dans E et avec X arbitraire, qui n'identifie jamais deux relations

différentes avec un même X . En particulier, les sous-ensembles vides de tous les E^X deviennent ainsi équivalents, et sont à considérer comme une même relation, notée $\emptyset$, à la première identification canonique près. De même, si l'on considère les X-relations E^X , la première identification canonique étendue par transitivité les identifie toutes (elle identifie, en effet, E^X et $E^{X'}$ avec $E^{X \cup X'}$), et il y a lieu de ne voir en elles, à cette identification près, qu'une seule relation (de E) notée I .

2° Soient C une équivalence dans X , et $X' = X/C$ l'ensemble des classes de cette équivalence. Soit $\eta_C : X \to X'$ l'application canonique de X sur X' . Si $P' : X' \to E$ est un X'-point de E , le composé $P = P' \circ \eta_C$ de P' et de η_C (écrit dans la notation de BOURBAKI) est un X-point de E , et

$$P' \to P = P' \circ \eta_C$$

est une injection de $E^{X'}$ dans E^X , qui induit une injection

$$r' \to r = \{P' \circ \eta_C \; ; \; P' \in r'\}$$

de l'ensemble des X'-relations de E dans celui des X-relations de E . Un X-point P est l'image $P' \circ \eta_C$ de quelque X'-point P' , si, et seulement si, $x \equiv y \pmod{C}$ implique $P.x = P.y$ (un tel point P sera dit <u>compatible</u> avec C). Une X-relation r est donc l'image par la même injection de quelque X'-relation r' , si, et seulement si, tout $P \in r$ est compatible avec C .

On appelle <u>deuxième identification canonique</u> (pour le couple X , C), l'identification des X'-relations arbitraires r' avec leurs images r par injection précédente. On dira qu'on la fait dans le sens <u>direct</u> ou <u>inverse</u>, selon qu'on passe de r' à r ou de r à r' .

Les <u>opérations fondamentales</u> qu'on va définir se partagent en plusieurs sous-familles :

(I) <u>Opérations booléennes infinitaires.</u>

(Ia) <u>Intersection infinitaire</u> $R \to \cap R$: Cette opération est définie pour les ensembles arbitraires R de X-relations dans E , et son résultat $\cap R$ est l'intersection des $r \in R$.

(Ib) <u>Réunion infinitaire</u> $R \to \cup R$: Cette opération est aussi définie pour les ensembles arbitraires R de X-relations dans E , et son résultat $\cup R$ est la réunion des $r \in R$.

(Ic) <u>Opposition</u> (ou <u>négation</u>) $r \to \neg r$: Cette opération est définie pour toute X-relation r dans E , et son résultat est la X-relation $\neg r = E^X . . r$,

dite anti-r .

Remarques.

(a) Pour certaines raisons qu'il n'est pas possible d'expliciter dans ce résumé, il est préférable de considérer l'intersection et la réunion infinitaires pas comme les opérations unaires définies sur la famille des ensembles de relations, mais comme opérations symétriques d'arité arbitraire sur les relations.

(b) Les opérations (Ia), (Ib), et (Ic), ne sont pas indépendantes : ainsi, si $\neg R$ désigne $\{\neg r ; r \in R\}$, on a $\cup R = \neg [\cap(\neg R)]$ et $\cap R = \neg [\cup(\neg R)]$. Mais l'opposition n'est pas une combinaison de l'intersection et de la réunion infinitaires.

(II) Projections (ou cylindrifications). - Pour tout couple $(X , \overline{X} \subseteq X)$, la $\overline{X}$-projection $r \to r_{\overline{X}}$ est définie comme suit :

Si $P : X \to E$ est un X-point de E , $P_{\overline{X}}$ sera, par définition, l'ensemble des X-points identifiés, par la première identification canonique, à la restriction $\overline{P} = \{x \to P.x ; x \in \overline{X}\}$ de P à $\overline{X}$; et, si r est une X-relation de E , on pose $r_{\overline{X}} = \bigcup_{P \in r} P_{\overline{X}}$. Autrement dit, $r_{\overline{X}}$ est l'ensemble des X-points P , dont la restriction à $\overline{X}$ coïncide avec celle de quelque point de r . Une X-relation r sera dite identique sur $X..\overline{X}$, si $r = r_{\overline{X}}$. Visiblement, les X-relations identiques sur $X..\overline{X}$ sont précisément celles que la première identification canonique identifie avec les $\overline{X}$-relations. Si $\overline{X}$ et $\overline{\overline{X}}$ sont des sous-ensembles de X tels que $\overline{X} \cap \overline{\overline{X}} \neq \emptyset$, on a $(r_{\overline{X}})_{\overline{\overline{X}}} = r_{\overline{X} \cap \overline{\overline{X}}}$, et cette égalité reste encore vraie quand $\overline{X} \cap \overline{\overline{X}} = \emptyset$, si l'on adopte la convention (pour $\overline{\overline{X}} = \emptyset$) $\emptyset_{\emptyset} = \emptyset$ et $r_{\emptyset} = I$ si $r \neq \emptyset$.

(III) Mutations (ou changements généralisés des noms de variables) $r \to r^{(\varepsilon)}$. - Avant de décrire ces opérations, applicables à certaines X-relations r de E , décrivons une classe particulière de ces opérations, celle des mutations simples (ou changements des noms de variables tout court).

Soient $\overline{X}$, $\overline{\overline{X}}$ deux sous-ensembles de X ayant une même cardinalité, et $\varepsilon : \overline{X} \to \overline{\overline{X}}$ une bijection de $\overline{X}$ sur $\overline{\overline{X}}$. Toute bijection ε de cette forme définit, comme suit, une mutation simple $r \to r^{(\varepsilon)}$:

Tout d'abord, le domaine de définition de cette opération est l'ensemble des X-relations r identiques sur $X..\overline{X}$. Si r est une telle relation (dans E), elle s'identifie, par première identification canonique, avec une $\overline{X}$-relation $\overline{r}$. Si $\overline{P}$ est un $\overline{X}$-point de E , $\overline{P}^{(\varepsilon)} = \overline{P} \circ \varepsilon^{-1}$ est un $\overline{\overline{X}}$-point de E , et

$$\overline{r}^{(\varepsilon)} = \{\overline{P}^{(\varepsilon)} ; \overline{P} \in \overline{r}\}$$

est une $\overline{\overline{X}}$-relation dans E . On définit $r^{(\varepsilon)}$ comme X-relation dans E , identifiée avec cette $\overline{\overline{X}}$-relation par la première identification canonique.

Pour définir les mutations générales, on part de la situation plus compliquée suivante : On a encore deux sous-ensembles $\overline{X}$, $\overline{\overline{X}}$ de X , mais, en plus, on se donne, sur ces ensembles, des relations d'équivalence $\overline{C}$, $\overline{\overline{C}}$ telles que les ensembles quotients $X' = \overline{X}/\overline{C}$ et $X'' = \overline{\overline{X}}/\overline{\overline{C}}$ aient une même cardinalité ; et, finalement, on se donne une bijection $\varepsilon : X' \to X''$. Chaque bijection ε de cette forme définit une mutation $r \to r^{(\varepsilon)}$.

Cette opération est définie pour les X-relations r , qui sont identiques sur $X..\overline{X}$ (donc s'identifient avec des $\overline{X}$-relations $\overline{r}$), et sont, en plus, telles que, pour les x , $y \in \overline{X}$, tout $P \in r$ prend une même valeur sur x et y $(P.x = P.y)$, si $x \equiv y \pmod{\overline{C}}$ (on appelle encore de tels points P <u>compatibles</u> avec $\overline{C}$, et la condition signifie que la $\overline{X}$-relation $\overline{r}$ identifiée avec r par la première identification canonique peut s'identifier, à son tour, avec une X'-relation r' par la seconde identification). Comme ε est une mutation simple pour les ensembles de variables X' , X'' , on obtient, en l'appliquant à r' , une X''-relation $r'' = r'^{(\varepsilon)}$, laquelle peut être identifiée, par la seconde identification canonique, à une $\overline{\overline{X}}$-relation $\overline{\overline{r}}$, qui, à son tour, s'identifie, par la première identification canonique, à une X-relation identique sur $X..\overline{\overline{X}}$. C'est cette dernière relation qui sera, par définition, $r^{(\varepsilon)}$.

On peut montrer qu'on obtient, à partir de la relation $I = E^X$, en lui appliquant des mutations convenables, les relations suivantes : pour tous x , $y \in X$, $x \neq y$, les <u>diagonales simples</u> $D_{x,y}$, qui sont les X-relations telles que $P \in D_{x,y} \iff P.x = P.y$; pour tout sous-ensemble Y de X , la <u>diagonale</u> D_Y , qui est la X-relation telle que $P \in D_Y$ a lieu si, et seulement si, $P.x$ a une même valeur pour tous les $x \in Y$; pour tout sous-ensemble Y de X , et pour toute équivalence C de Y , la <u>multidiagonale</u> $I^{(C)}$, qui est la X-relation telle que $P \in I^{(C)}$ si, et seulement s'il est compatible avec C , autrement dit si $x \equiv y \pmod{C}$ implique $P.x = P.y$.

On appelle <u>opérations fondamentales directes</u>, toutes les opérations fondamentales sauf la négation $\neg$, autrement dit, l'intersection et la réunion infinitaires, toutes les projections et toutes les mutations, auxquelles on ajoute, toutefois, les opérations nullaires, qui consistent en l'adjonction des relations constantes $\not\in$ et I (il est inutile d'inclure ces opérations unaires parmi les opérations fondamentales quelconques, car elles en sont déjà des combinaisons : en effet, pour toute relation r , on a $\not\in = r \cap (\neg r)$ et $I = r \cup (\neg r)$).

On appelle type d'un X-point P, l'équivalence $T(P)$ de X telle que $x \equiv y \pmod{T(P)} \iff P.x = P.y$. Un X-point P est dit semi-normal, si $T(P)$ est l'équivalence discrète de X, autrement dit, si P est injectif. Il est dit normal, si, en plus, $P.X = E$, c'est-à-dire s'il est une bijection de X à E (ce qui implique $\operatorname{card} X = \operatorname{card} E$). Une X-relation r est dite semi-régulière, s'il existe un $P \in r$ tel que tout $P' \in r$ soit compatible avec $T(P)$, et l'ensemble de tels points $P \in r$ (qui ont un même type, qui sera appelé le type de r, et sera noté $T(r)$) est appelé la tête de r, et est noté $t(r)$.

Si r est une X-relation, on peut la représenter comme réunion de X-relations semi-régulières, dont chacune s'obtient à partir de r par application (itérée) de seules opérations fondamentales directes : $r = \bigcup_{P \in r} r_P$, où $r_P = r \cap I^{(T(P))}$.

Une relation semi-régulière r est dite régulière, si $t(r) = r$. On peut montrer que l'ensemble $I^{(C)*}$ des X-points de E de type C, où C est une équivalence de X, qui est la plus grande X-relation régulière de E de type C, s'obtient à partir de I par une combinaison des opérations fondamentales, mais pas par une combinaison des opérations fondamentales directes.

Quand E et X sont finis, il n'y a donc qu'un nombre fini des $r \subseteq E^X$ distinctes, toute intersection ou réunion infinie de tels r coïncide avec celle, convenable, d'un nombre fini d'entre eux, et on peut remplacer, dans ce cas, les opérations fondamentales par les opérations strictement finitistes. Si l'on considère les structures de premier ordre comme modèles du calcul des prédicats avec égalité, il se trouve que ces restrictions finitistes des opérations fondamentales sont des combinaisons des opérations (réalisées sur le modèle) du calcul des prédicats et de l'opération nullaire, qui consiste en l'adjonction du prédicat " $x = y$ " d'égalité, et que, vice versa, elles engendrent ces opérations. Quant aux restrictions analogues des opérations fondamentales directes, on peut montrer qu'elles engendrent les mêmes opérations que $\&$, $\vee$, $(\exists x)$ (par contre, sont exclues $\neg$ et $(\forall x)$), les substitutions des variables d'objet et l'adjonction d'égalité. Pour cette raison, pour E fini, les résultats de la théorie et de l'endothéorie de Galois abstraites peuvent être formulés comme résultats de la théorie des modèles. Et, dans le cas général, le cadre de ces théories peut être considéré comme théorie des modèles d'un analogue, avec des expressions infinies, du calcul des prédicats avec égalité, ou d'une certaine partie "positive" de ce calcul. D'ailleurs, on construit, à l'aide de certains arbres infinis, le langage propre de la théorie de Galois abstraite, permettant d'exprimer toutes ses expressions dérivées, en un sens infinitiste raisonnable, des opérations fondamentales.

3. Théorie de Galois abstraite et ses quelques développements.

E étant un support, soit X un ensemble de variables tel que card X $\geqslant$ card E + 1. Un ensemble R de X-relations dans E sera dit logiquement fermé, s'il l'est par rapport à toutes les opérations fondamentales (autrement dit, chaque fois qu'une opération fondamentale est appliquée à un élément ou à un sous-ensemble de R auquel elle est applicable, son résultat appartient à R). On montre que l'intersection d'une famille d'ensembles logiquement fermés est encore un ensemble logiquement fermé, d'où il résulte que tout ensemble R de X-relations dans E possède le plus petit surensemble logiquement fermé R_f, dit sa fermeture logique. Deux X-structures $S = (E , R)$ et $S' = (E , R')$ dans E seront dites équivalentes (notation : $S \backsim S'$), si $R_f = R'_f$; et on dira que S est plus faible que S' (notation : $S \prec S'$ ou $S' \succ S$), si $R_f \subset R'_f$.

Soit $d : E \to E'$ une application de E, et soient P, r, R, $S = (E , R)$, un X-point, une X-relation, un ensemble de X-relations, et une X-structure dans E. On étendra d à ces objets en posant $d.P = d \circ P$ (notation de BOURBAKI), $d.r = \{d.P ; P \in r\}$, $d.R = \{d.r ; r \in R\}$, $d.S = (E , d.R)$. Si $\Delta : E \to E$ est une autoapplication de E, on dit que Δ laisse stable une relation r dans E, si $\Delta.r \subseteq r$. On dit que Δ préserve r, s'il laisse stable à la fois r et $\neg r$. En particulier, si σ est une permutation (c'est-à-dire bijection) de E, σ préserve r si, et seulement si, $\sigma.r = r$. Si $S = (E , R)$ est une structure, l'ensemble $G_{E/S}$ des permutations σ de E préservant tout $r \in R$ est un groupe de permutations, dit le groupe de Galois par rapport à S (ou de E/S). On démontre les deux théorèmes suivants, qui jouent un rôle fondamental dans la théorie :

THÉORÈME d'équivalence (de la théorie de Galois abstraite). - On a $S \backsim S'$ (où S, S' sont deux X-structures dans E), si, et seulement si, $G_{E/S} = G_{E/S'}$.

THÉORÈME d'existence (de la théorie de Galois abstraite). - Pour tout groupe de permutations g de E, il existe une X-structure S de E telle que $g = G_{E/S}$.

On a aussi $S \prec S' \iff G_{E/S} \supset G_{E/S'}$.

Quand E est fini, on peut satisfaire à la condition card X $\geqslant$ card E + 1 en prenant X également fini. Dans ce cas, le théorème d'équivalence peut se formuler comme suit, en termes de la théorie des modèles :

Considérons un modèle d'un ensemble fini de prédicats (avec un ensemble vide d'axiomes) avec un support fini E. Alors, une relation de E correspond à un prédicat s'exprimant, à partir des prédicats primitifs, par une expression du

calcul des prédicats avec égalité, si, et seulement si, elle est préservée par toutes les permutations de E qui préservent toutes les relations qui représentent, dans le modèle, ces prédicats primitifs.

En vertu de la première identification canonique, une X-structure $S = (E , R)$ peut être considérée, pour tout $X' \supset X$, comme une X'-structure, dont toutes les relations $r \in R$ sont identiques sur $X'..X$. Ainsi, deux structures $S = (E , R)$ et $S' = (E , R')$ dans E, mais ayant leurs ensembles de coordonnées respectifs X , X' différents, peuvent être considérées toutes les deux comme X''-structures pour tout $X'' \supseteq X \cup X'$. En particulier, si card $X'' \geqslant$ card $E + 1$, ces structures sont équivalentes si, et seulement si, $G_{E/S} = G_{E/S'}$, et cette dernière condition ne dépend pas du choix de X''. Ainsi, dira-t-on que S et S' sont équivalentes si elles le sont pour quelque X'' de la forme précédente, ce qui définit une équivalence dans la classe des structures (de 1er ordre) de E. Les classes de cette équivalence seront appelées <u>corps-abstraits</u>. Ainsi, un corps abstrait K est une classe de structures S ayant un même groupe de Galois $G_{E/S}$, qui sera aussi noté $G_{E/K}$, et $K \to G_{E/K}$ est la bijection canonique de l'ensemble des corps abstraits de E sur celui des sous-groupes du groupe symétrique (c'est-à-dire celui de toutes les bijections) $S(E)$ de E. Un corps abstrait peut être aussi identifié avec une classe de relations dans E : on posera $r \in K$, s'il existe une structure $S = (E , R)$ dans K (considéré comme classe de structures) telle que $r \in R$. On voit facilement que $r \in K$ a lieu si, et seulement si, r est préservée par tous les $\sigma \in G_{E/K}$. Un corps abstrait k est dit un <u>sous-corps</u> du corps abstrait K, si les structures de k sont plus faibles que celles de K (autrement dit, si $G_{E/k} \supset G_{E/K}$).

K , K' étant deux corps abstraits (dont les supports E , E' ne sont pas supposés égaux), tels qu'il est définie une bijection η de la classe des relations appartenant à K sur celle des relations appartenant à K', cette bijection est dite un <u>isomorphisme</u> de K sur K', si $r \to \eta.r$ est un isomorphisme par rapport aux opérations fondamentales. Le cas évident d'un tel isomorphisme est fourni par le <u>transport des structures</u> : soient $S = (E , R)$ une structure dans E, et $K = K(S)$ le corps abstrait qu'elle définit (c'est-à-dire la classe des structures qui lui sont équivalentes). Si $d : E \to E'$ est une bijection de E sur un ensemble E', $r \to d.r$, $S \to d.S$ et $K \to d.K = K(d.S)$ sont dits les <u>transports</u> des relations, des structures, et des corps abstraits de E par la bijection d (d'ailleurs, ces définitions restent valables quand d est une application quelconque de E dans E'). Il est visible que le transport $(d) : r \to d.r$ des $r \in K$ est un isomorphisme de K sur $K' = d.K$. Mais on peut prouver :

THÉORÈME d'isomorphie. - Pour tout isomorphisme $\eta : r \to r'$ d'un corps abstrait K dans E sur un corps abstrait K' dans E' , il existe une bijection $d : E \to E'$ telle que η coïncide avec le transport $(d) : r \to d.r$ par d .

Si $e \in E$, et si x est une variable, notons $(x ; e)$ la $\{x\}$-relation dans E telle que $P \in (x ; e) \iff P.x = e$. Si K est un corps abstrait, e est dit un élément rationnel de K , s'il est préservé par tout $\sigma \in G_{E/K}$. Ceci a lieu si, et seulement si, σ préserve $(x ; e)$, où x est arbitrairement fixé, autrement dit, si, et seulement si, $(x ; e) \in K$. L'ensemble des éléments rationnels de K est dit son domaine de rationalité.

Etant donné un corps abstrait $k = K(S_0)$, où $S_0 = (E , R_0)$, et R étant un ensemble de relations dans E , $K = K(S)$, où $S = (E , R_0 \cup R)$, sera dit l'extension abstraite de k (qui sera dit le corps abstrait de base), obtenue par l'adjonction de R , et sera noté $k(R)$. En particulier, $k((x ; e))$ et, en général, $k(\{(x ; a) ; a \in A\})$, où $A \subseteq E$, ne dépendent pas du choix de x , et seront notés $k(e)$ et $k(A)$ respectivement, et $k(A)$ sera appelé l'extension multiplicitaire du corps abstrait k , obtenue par l'adjonction de l'ensemble $A \subseteq E$. La théorie de Galois multiplicitaire est l'étude des extensions multiplicitaires d'un corps abstrait donné, en particulier la recherche de la caractérisation des domaines de rationalité des $k(A)$ à partir des k et A (premier problème), et l'étude de la famille $\{G_{E/k(A)} ; A \subseteq E\}$ de sous-groupes de $G_{E/k}$ (deuxième problème). On peut prouver que :

THÉORÈME fondamental de la théorie de Galois multiplicitaire. - Toute relation du corps abstrait $k(A)$, où k est un corps abstrait de E , et où $A \subseteq E$, est une réunion de relations (qui appartiennent sûrement à $k(A)$) de la forme suivante :

$$r' = [r \cap [\cap\{(x ; f.x) ; x \in Y\}]]_{\overline{X}} ,$$

où, si $X = \overline{X} \cup Y$, r est une X-relation appartenant à k (on peut, même, la supposer irréductible parmi de telles relations, autrement dit, supposer que, si une X-relation appartenant à k est $\subseteq r$, elle est égale à r ou à $\emptyset$), et $f : Y \to A$ est une application de Y dans A .

Ce théorème permet de donner une réponse de principe au premier problème. Soit r une X-relation dans E , où $\text{card } X \geqslant 1$, et soient $y \in X$ et $\overline{X} = X..\{y\}$. Définissons, à partir de r et de y , une $\overline{X}$-opération partielle ω_y^r dans E , autrement dit, une application d'une partie convenable D_y^r de $E^{\overline{X}}$ dans E . D_y^r est définie comme la partie de $r_{\overline{X}}$ formée des $\overline{X}$-points $\overline{P} \in r_{\overline{X}}$ tels qu'il existe un seul $P \in r$, dont la restriction à $\overline{X}$ soit $\overline{P}$ (cette $\overline{X}$-relation est facilement exprimable à partir de r à l'aide des opérations fondamentales), et, si

$\overline{P} \in D_y^r$, $\omega_y^r.\overline{P}$ est défini par la condition que $P \in r$ et $P_{\overline{X}} = \overline{P}$ impliquent $P.y = \omega_y^r.\overline{F}$. Alors, le domaine de rationalité de $k(A)$ est la fermeture de A par rapport aux opérations ω_y^r , où r parcourt les X-relations appartenant à k , où X est un ensemble fixé de coordonnées tel que card X = card E , et y est un élément fixé de X (on peut supposer, en plus, que r ne parcourt que des relations X-irréductibles de k).

Toutefois, cette solution de principe est peu satisfaisante dans les situations concrètes, car le corps abstrait k est en général défini par la donnée de la structure $S_0 = (E , R_0)$, et les relations appartenant à R_0 sont, le plus souvent, d'arité finie. On aimerait avoir un critère analogue, mais où les relations du corps abstrait k auraient été remplacées par celles de structure de base S_0 . Effectivement, il existe une large classe de structures, dites structures éliminatives (et qu'il serait trop long de définir ici), où cela est possible. En particulier, la structure, qui sert de cadre à la théorie de Galois classique, est éliminative si l'on prend comme son ensemble des relations R_0 , celui des "égalités polynomiales" $f = 0$, où f parcourt l'anneau $k[X_1 , X_2 , \dots , X_n , \dots]$ des polynômes d'une suite dénombrable $X_1 , X_2 , \dots , X_n , \dots$ de variables à coefficients dans le corps (au sens usuel) de base k . On montre que la fermeture de A par rapport aux opérations ω_y^r , qui dérivent de ces relations $r = (f = 0)$, coïncide avec celle de $A \cup k$ par rapport aux opérations $x + y$, xy , x^{-1} et (éventuellement) $\sqrt[p]{x}$, indiquées dans le paragraphe 1.

4. Endothéorie de Galois abstraite.

Soit E un support, et soit X un ensemble de variables tel que card $X \geqslant$ card E . Un ensemble R de X-relations dans E sera dit directement fermé, s'il est fermé par rapport à toutes les opérations fondamentales directes. On montre que l'intersection d'une famille d'ensembles directement fermés de X-relations dans E l'est encore. Par suite, tout ensemble R de X-relations dans E possède le plus petit sur-ensemble R_{df} directement fermé, qui est dit sa fermeture directe. Si $S = (E , R)$ et $S' = (E , R')$ sont deux X-structures dans E , elles seront dites directement équivalentes (notation : $S \sim_d S'$), si $R_{df} = R'_{df}$, et on dira que S est directement plus faible que S' (notation : $S <_d S'$ ou $S' >_d S$), si $R_{df} \subset R'_{df}$.

$S = (E , R)$ étant une structure dans E , l'ensemble $D_{E/S}$ des autoapplications $A : E \to E$ de E , qui laissent stable toute relation $r \in R$, est un demi-groupe par rapport à la composition des applications, auquel appartient l'identité 1_E de E . Ce demi-groupe sera dit le demi-groupe de stabilité par rapport à S (ou de

E/S). Les deux théorèmes suivants sont les analogues, dans l'endothéorie de Galois abstraite, des théorèmes du même nom de la théorie de Galois abstraite, et jouent un rôle aussi important.

THÉORÈME d'équivalence directe. - Si S , S' sont deux X-structures dans E , où card X $\geqslant$ card E , on a $S \backsim_d S'$ si, et seulement si, $D_{E/S} = D_{E/S'}$.

On peut, d'ailleurs, prouver que, plus généralement, on a $S <_d S'$ si, et seulement si, $D_{E/S} \supset D_{E/S'}$.

THÉORÈME d'existence de l'endothéorie de Galois abstraite. - Si card X $\geqslant$ card E , tout demi-groupe D d'autoapplications de E tel que $1_E \in D$ est de la forme $D_{E/S}$, où S est une X-structure dans E convenable.

Idée de démonstration de ces théorèmes.

(a) On considère l'ensemble R_D (où D est un demi-groupe d'autoapplications de E tel que $1_E \in D$) des X-relations r préservées par tout $\Delta \in D$. On prouve que, si l'on applique n'importe laquelle opération fondamentale directe aux relations laissées stables par une autoapplication Δ de E , Δ laisse stable aussi le résultat de l'opération, ce qui montre que R_D est directement fermé. Appelons D-orbite d'un point (qui n'est pas forcément un X-point) P de E , l'ensemble $D.P = \{\Delta.P \ ; \ \Delta \in D\}$, considéré à la première identification près. On montre facilement qu'une X-relation r appartient à S_D si, et seulement si, elle est une réunion de D-orbites de X-points de E , et que, si P est un point surjectif, l'ensemble des autoapplications de E , qui laissent stable la D-orbite D.P de P , coïncide avec D . Ceci montre, en particulier, que, si $S_D = (E , R_D)$, D coïncide avec le demi-groupe de stabilité de E/S_D , ce qui prouve le théorème d'existence. D'autre part, si $D = D_{E/S}$, on a, visiblement, $R \subseteq R_D$, d'où il résulte que $R \subseteq R_{df} \subseteq (R_D)_{df} = R_D$. Comme D est à la fois l'ensemble de toutes les autoapplications de E , qui laissent stable toute $r \in R$, et l'ensemble de celles qui laissent stable toute $r \in R_D$, il est aussi l'ensemble de celles qui laissent stable toute $r \in R_{df}$. Par suite, $S = (E , R) \backsim_d S' = (E , R')$, autrement dit, $R_{df} = R'_{df}$, implique $D_{E/S} = D_{E/S'}$.

(b) Soit $\widetilde{X}$ un sous-ensemble de X tel que card $\widetilde{X}$ = card E (un tel $\widetilde{X}$ existe, en vertu de card X $\geqslant$ card E), et soit $\widetilde{P} : \widetilde{X} \to E$ un $\widetilde{X}$-point normal. On a $D.\widetilde{P} \in R_D$ (où $D = D_{E/S}$). Mais, si P est un X-point arbitraire, on peut montrer que la D-orbite D.P de P s'obtient à partir de celle $D.\widetilde{P}$ de $\widetilde{P}$ par les opérations fondamentales directes. En effet (en adoptant la notation de BOURBAKI), posons $\widetilde{X}_P = (\widetilde{P}^{-1} \circ P).X = \widetilde{P}^{-1}.(P.X)$. On va définir, à partir des points $\widetilde{P}$ et P ,

une certaine mutation $\varepsilon = \varepsilon_{\widetilde{P},P}$. On va, d'abord, poser $\overline{X} = X_P$,

$\overline{C}$ = équivalence discrète de $\overline{X}$, $\overline{\overline{X}} = X$,

$\overline{\overline{C}} = T(P)$,

et, si $x \in \overline{X}$, on posera $\varepsilon.x$ égal à l'ensemble des $y \in X$ tels que $P.y = \widetilde{P}.x$ (puisque $\overline{X} = \widetilde{X}_P$, cet ensemble n'est pas vide, et il est une classe (mod $T(P)$) , donc un élément de $X'' = \overline{\overline{X}}/\overline{\overline{C}} = X/T(P)$). On montre facilement que

$$P = (\widetilde{P}_{\widetilde{X}_P})^{(\varepsilon_{\widetilde{P},P})} \qquad \text{et} \qquad \widetilde{P}_{\widetilde{X}_P} = P^{(\varepsilon^{-1}_{\widetilde{P},P})} ,$$

et que ces égalités commutent avec toute autoapplication Λ de E , d'où il résulte, en particulier, que

$$D.P = [(D.\widetilde{P})_{\widetilde{X}_P}]^{(\varepsilon_{\widetilde{P},P})} .$$

Par suite, toute $r \in R_D$ s'obtient de $D.\widetilde{P}$ par application des opérations fondamentales directes, et, ainsi, on a $\{D.\widetilde{P}\}_{df} = R_D = (R_D)_{df}$.

(c) Supposons que $D_{E/S} = D_{E/S'} = D$. Alors, R et R' sont des sous-ensembles de R_D , et il suffit de prouver, pour chacun de ces ensembles, la coïncidence de sa fermeture directe avec R_D , pour achever la démonstration du théorème d'équivalence. Si l'on considère, dans ce but, par exemple R , il suffit, en vertu de (b), de prouver que $D.\widetilde{P} \in R_{df}$. On le fait en construisant explicitement $D.\widetilde{P}$, à l'aide des opérations fondamentales directes, à partir des $r \in R$. On commence par remplacer toute $r \in R$ par l'ensemble $\{r_P \ ; \ P \in r\}$ des relations semi-régulières, dont r est la réunion, et dont chacune s'obtient de r (comme on l'a vu à la fin du paragraphe 2) par opérations fondamentales directes. Soit R^0 la réunion de tous ces ensembles de relations (donc $R^0 \subseteq R_{df}$). On considère la relation

$$r^0 = \bigcap_{r \in R^0} \bigcap_{P \in t(r)} r^{(\varepsilon^{-1}_{\widetilde{P},P})} ,$$

et, en se basant sur les propriétés indiquées des $\varepsilon^{-1}_{\widetilde{P},P}$ (et des mutations en général), on prouve que r^0 est précisément l'orbite cherchée $D.\widetilde{P}$.

Déduction des théorèmes d'équivalence et d'existence de la théorie de Galois abstraite à partir de ceux de l'endothéorie. - Si G est un groupe de permutations de E , une relation r , qui est laissée stable par tous les $\sigma \in G$, est aussi préservée par ces σ . Ainsi, si S est une X-structure dans E (qui existe, si card $X \geqslant$ card E) telle que $G = D_{E/S}$, on a aussi $G = G_{E/S}$, ce qui démontre le théorème d'existence de la théorie de Galois abstraite. En ce qui concerne le

théorème d'équivalence, remarquons que, si une permutation laisse stables r et $\neg r$, elle préserve r. Par suite, si $S = (E, R) = (E, \neg R)$, $G_{E/S}$ est l'intersection $D_{E/S} \cap S(E)$ de $D_{E/S}$ avec le groupe symétrique $S(E)$ de E. Les parties (a) et (b) du raisonnement précédent restent valables, si l'on y remplace les opérations fondamentales directes par toutes les opérations fondamentales quelconques, la fermeture directe par la fermeture logique, la stabilité des relations par leur préservation, les autoapplications quelconques de E par ses permutations, les demi-groupes par les groupes, l'équivalence directe des structures par leur équivalence tout court, etc. Donc, pour achever la démonstration du théorème d'équivalence de la théorie de Galois abstraite, il suffit de construire la G-orbite $G.\widetilde{P}$ de $\widetilde{P}$, où $G = G_{E/S}$, à partir des $r \in R$, à l'aide des opérations fondamentales quelconques. Commençons par remplacer R par $R \cup (\neg R) \subseteq R_f$, car, puisque $\neg (R \cup (\neg R)) = R \cup (\neg R)$, on a $G = G_{E/(E,R\cup(\neg R))} = D_{E/(E,R\cup(\neg R))} \cap S(E)$. En vertu du théorème d'équivalence de l'endothéorie, on peut construire à partir de $R \cup (\neg R)$, à l'aide des opérations fondamentales (même directes seulement), la D-orbite $D.\widetilde{P}$ de $\widetilde{P}$, où $D = D_{E/(E,R\cup(\neg R))}$, et $G.\widetilde{P}$ est donc l'ensemble des points normaux de $D.\widetilde{P}$. Pour éliminer les $\widetilde{X}$-points non normaux de $D.\widetilde{P}$, on procède par deux étapes, ayant pris auparavant, quand on a construit $r^0 = D.\widetilde{P}$, la précaution de choisir comme $\widetilde{X}$ un sous-ensemble propre de X (ceci est possible à cause de l'hypothèse $\operatorname{card} X \geqslant \operatorname{card} E + 1$). Désignons par $C_0(Y)$ l'équivalence discrète sur l'ensemble (arbitraire) Y, et posons $r^{00} = r^0 \cap I^{(C_0(X))^*}$. Alors, r^{00} est l'ensemble des points de r^0, dont le type est $C_0(X)$, c'est-à-dire celui de ses points semi-normaux, ce qui élimine déjà ceux qui ne le sont pas. Soit $x \in X..\widetilde{X}$ (un tel x existe, car, par hypothèse, $X..\widetilde{X} \neq \emptyset$). Un $\widetilde{X}$-point injectif P' peut se prolonger en un $(\widetilde{X} \cup \{x\})$-point injectif, si, et seulement s'il n'est pas bijectif. Par suite, $[r^{00} \cap I^{(C_0(\widetilde{X}\cup\{x\}))^*}]_{\widetilde{X}}$ est l'ensemble des points non bijectifs, c'est-à-dire non normaux, de r^{00}, et

$$r^{000} = r^{00} \cap (\neg [r^{00} \cap I^{(C_0(\widetilde{X}\cup\{x\}))^*}]_{\widetilde{X}})$$

est l'ensemble des points normaux de r^{00} (donc aussi de r^0), et, par suite, coïncide avec $G.\widetilde{P}$.

Si E est fini, et si l'on prend un X fini tel que $\operatorname{card} X \geqslant \operatorname{card} E$, on peut, comme dans la théorie de Galois abstraite, donner au théorème d'équivalence de l'endothéorie l'expression suivante, en termes de la théorie des modèles :

Etant donné un modèle de support E pour un système fini de prédicats primitifs, dont les variables d'objets appartiennent à X, une X-relation dans E représente dans le modèle un prédicat, obtenu à partir des prédicats primitifs et du

prédicat d'égalité par les opérations (du calcul des prédicats) : $\&$, $\vee$, les quantificateurs existentiels et les substitutions des variables d'objet, si, et seulement si, toute autoapplication de E , qui laisse stable toute relation représentant, dans le modèle, un des prédicats primitifs du système, laisse stable la relation considérée.

On définit la notion générale d'équivalence directe de deux structures S , S' dans E (dont les ensembles des variables X , X' peuvent être différents), et la notion d'endocorps abstrait de manière analogue à celle de la théorie de Galois abstraite : On considère S et S' comme X''-structures, où $X'' \supseteq X \cup X'$ est tel que card $X'' \geqslant$ card E , et on considère S et S' comme directement équivalentes si elles le sont en tant que X''-structures. Comme ceci a lieu, indépendamment du choix de X'' , si, et seulement si, $D_{E/S} = D_{E/S'}$, cette définition est cohérente. Un endocorps abstrait n'est pas autre chose qu'une classe de cette équivalence, et il est dit défini par toute structure S , qui appartient à cette classe, auquel cas on l'écrira $K_e(S)$. Toutes les structures S , qui définissent un endocorps abstrait donné K , ont un même demi-groupe de stabilité $D_{E/S}$, qui sera aussi noté $D_{E/K}$, et dit le demi-groupe de stabilité par rapport à K (ou de E/K), et $K \to D_{E/K}$ est une bijection de l'ensemble des endocorps abstraits de E sur celui des demi-groupes D d'autoapplications de E tels que $1_E \in D$. On peut aussi identifier des endocorps abstraits avec des classes de relations. On dira qu'une relation r de E appartient à un endocorps abstrait K (ou est une relation de K), s'il existe une structure $S = (E , R)$ telle que $K = K_e(S)$ et $r \in R$. Visiblement, on a $r \in K$ si, et seulement si, tous les $A \in D_{E/K}$ laissent r stable. Un endocorps abstrait $k = K_e(S_0)$ est dit un sous-endocorps de l'endocorps abstrait K (et K est dit une endoextension de k), si $S_0 <_d$ ou $\backsim_d S$ (si $K \neq k$, on dira que k est un sous-endocorps propre de K). On définit, comme pour les corps abstraits, l'endoextension $k(R)$ de k obtenue par l'adjonction d'un ensemble R de relations, et l'endoextension multiplicitaire $k(A)$ de k obtenue par l'adjonction d'un $A \subseteq E$.

Comme $S \backsim_d S'$ implique $S \backsim S'$, on voit que $K_e(S) \to K(S)$ est une surjection canonique de l'ensemble des endocorps abstraits de E sur celui des corps abstraits de E . Mais, d'autre part, un corps abstrait K de E , considéré comme classe de relations, coïncide avec l'endocorps abstrait K' de E , tel que $D_{E/K'} = G_{E/K}$: en effet, une relation r , qui est laissée stable par tous les éléments σ du groupe de permutations $G = G_{E/K} = D_{E/K'}$ de E , donc aussi par leurs inverses, est préservée par tous ces σ . Ainsi, l'application $K \to K'$ est une injection canonique de l'ensemble des corps abstraits de E dans celui de ses endocorps abstraits.

Il existe, dans l'endothéorie de Galois abstraite, un <u>théorème d'homomorphie</u> analogue à celui d'isomorphie de la théorie de Galois abstraite. Afin de le formuler, introduisons certaines notions :

1° Soient D un demi-groupe d'autoapplications de E, et $d : E \to E'$ une surjection de E sur E'. On dira que d est une <u>représentation</u> de D, si la condition suivante est satisfaite : Si $x, y \in E$ sont tels que $d.x = d.y$, alors, pour tout $\xi \in D$, on a aussi $d.(\xi.x) = d.(\xi.y)$. S'il en est ainsi, $d.(\xi.x)$ (pour un $\xi \in D$ fixé) ne dépend que de $d.x$, et $d.x \to d.(\xi.x)$ est une autoapplication de E', notée ξ^d, et dite transformée de ξ par d ; et l'application $\xi \to \xi^d$ est un homomorphisme de D sur son image D^d.

2° Si k est sous-endocorps d'un endocorps abstrait K, et si r est une relation appartenant à K, l'intersection de toutes les relations appartenant à k contenant r est la plus petite relation appartenant à k, qui la contient. On note cette relation $N_{K/k}(r)$, et on l'appelle la <u>norme de</u> K <u>à</u> k (ou <u>dans</u> K/k) <u>de</u> r.

3° Soient K, K' deux endocorps abstraits des supports pas forcément égaux E, E'. Une surjection η de la classe des relations appartenant à K sur celle des relations appartenant à K' sera dite un <u>homomorphisme</u> de K sur K', si elle satisfait aux conditions suivantes :

(I) <u>Pour tout ensemble</u> R <u>de relations appartenant à</u> K, $\eta.(\cup R) = \cup(\eta.R)$ (R <u>étant un ensemble arbitraire de relations,</u> $\eta.R$ <u>signifie</u> $\{\eta.r ; r \in R\}$;

(II) <u>Si</u> r <u>est une relation</u> $\in K$, <u>et si</u> R' <u>est un ensemble de relations appartenant à</u> K' <u>tel que</u> $\eta.r = \cup R'$, <u>il existe une application (forcément injective)</u> θ <u>de</u> R' <u>dans la classe des relations appartenant à</u> K, <u>telle que, pour toute</u> $r' \in R'$, <u>on ait</u> $\eta.(\theta.r') = r'$, <u>et que</u> $r = \cup\{\theta.r' ; r' \in R'\}$;

(III) <u>Pour toute relation</u> $r \in K$, <u>et pour tout ensemble de coordonnées</u> X, <u>on a</u> $\eta.r_X = (\eta.r)_X$;

(IV) <u>Pour toute relation</u> $r \in K$, <u>et pour toute mutation</u> ε <u>définie pour</u> r, $(\eta.r)^{(\varepsilon)}$ <u>est définie, et on a</u> $\eta.r^{(\varepsilon)} = (\eta.r)^{(\varepsilon)}$.

Si K est un endocorps abstrait de E, on voit immédiatement que les deux sortes d'applications suivantes sont des homomorphismes de K :

1° Soit d une représentation du demi-groupe de stabilité $D = D_{E/K}$ de E/K. Alors, $(d) : r \to d.r$ est un homomorphisme de K sur l'endocorps abstrait $d.K$ de $E' = d.E$ (on a, d'ailleurs, $D_{E'/d.K} = (D_{E/K})^d$).

2° Soit k un sous-endocorps de K. Alors, l'application $N_{K/k} : r \to N_{K/k}(r)$ est un homomorphisme de K sur k. Mais on a :

THÉORÈME d'homomorphie. - Si η est un homomorphisme d'un endocorps abstrait K de E sur un endocorps abstrait K' de E' , il existe une surjection d : E→E' de E sur E' , qui est une représentation de $D = D_{E/K}$, et un sous-endocorps k' de K' = d.K , tels que $\eta = N_{d.K/k'} \circ (d)$, autrement dit, que, pour toute relation $r \in K$, on ait $\eta.r = N_{K/k}(d.r)$.

Le théorème fondamental de la théorie de Galois multiplicitaire reste textuellement vrai, si l'on y remplace l'hypothèse que k est un corps abstrait par celle qu'il est un endocorps abstrait (il serait, d'ailleurs, plus juste de parler dans ce cas plus général du théorème fondamental de l'endothéorie de Galois multiplicitaire).

BIBLIOGRAPHIE

[1] KRASNER (Marc). - Une généralisation de la notion de corps, J. Math. pures et appl., 9e série, t. 9, 1938, p. 367-385.

[2] KRASNER (Marc). - Généralisations et analogues de la théorie de Galois, Association Française pour l'Avancement des Sciences, 64e session, Congrès de la Victoire [1945. Paris], Mathématiques, p. 54-58. - Paris, Intermédiaire des Recherches mathématiques, 1947 (Supplément au fascicule 9 de l'Intermédiaire des Recherches mathématiques).

[3] KRASNER (Marc). - Généralisation abstraite de la théorie de Galois, Colloques internationaux du C. N. R. S. : Algèbre et théorie des nombres [24. 1949. Paris], p. 163-168. - Paris, Centre national de la Recherche scientifique, 1950.

[4] KRASNER (Marc). - Généralisation abstraite de la théorie de Galois, Proceedings of the international Congress of Mathematicians [1950. Cambridge], vol. 1, p. 331-332. - Providence, American mathematical Society, 1952.

[5] KRASNER (Marc). - Les algèbres cylindriques, Réunion des Mathématiciens d'expression latine [1957. Nice], Bull. Soc. math. France, t. 86, 1958, p. 315-319.

[6] KRASNER (Marc). - Endothéorie de Galois abstraite, Congrès international des Mathématiciens [1966. Moscou], Résumés 2 : Algèbre, p. 61. - Moskva, ICM, 1966.

[7] KRASNER (Marc). - Théorie de Galois classique et abstraite, Cours de 3e cycle donné à la Faculté des Sciences de Paris, 1966/67, chap. VI : Théorie et endothéorie de Galois abstraites, 36 p. (Notes miméographiées, hors de commerce).

(Texte reçu en décembre 1970)

Marc KRASNER
1 rue Ernest Gouin
75 - PARIS 17