

Prop. 5: Supposons que \bar{P} est séparable. Alors l'action à droite de $\text{Gal}_{\mathbb{Q}}(P)$ sur l'ensemble $\text{Hom}_{\text{an}}(A, L)$ des morphismes d'anneaux $A \rightarrow L$ définie par

$\varphi \cdot \sigma = \varphi \circ \sigma$, $\varphi \in \text{Hom}_{\text{an}}(A, L)$, $\sigma \in \text{Gal}_{\mathbb{Q}}(P)$,
est simplement transitive.

$$\begin{array}{ccc} A & \xrightarrow{\sigma} & A \\ & \searrow \varphi \circ \sigma & \downarrow \varphi \\ & & L \end{array}$$

Reques: 1) Tout morph. d'anneaux $A \xrightarrow{\varphi} L$ est surjectif car \bar{P} se scinde dans $\text{Im} \varphi$.

2) Si \bar{P} est séparable, alors P l'est aussi car $\text{disc}(\bar{P}) \in \mathbb{F}_p$ est la réduction modulo p de $\text{disc}(P) \in \mathbb{Z}$.

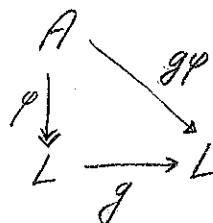
Dém. de la prop.: Soit $\varphi: A \rightarrow L$ un morphisme d'anneaux. Soient $\Omega \subset A$ l'ensemble des racines de P et $\bar{\Omega} \subset L$ l'ensemble des racines de \bar{P} . Comme \bar{P} se scinde dans $\text{Im} \varphi$, φ induit une surjection $\Omega \rightarrow \bar{\Omega}$. Or P et \bar{P} sont séparables et de même degré. Donc Ω et $\bar{\Omega}$ ont même cardinal et φ induit une bijection $\Omega \rightarrow \bar{\Omega}$. Donc si $\varphi \circ \sigma = \varphi$, alors $\sigma|_{\Omega}$ est l'identité et σ est l'identité. Donc l'action est libre. Chacune de ses orbites est de cardinal $|\text{Gal}_{\mathbb{Q}}(P)| = [E:K]$ et il existe au moins une orbite (Prop. 3). Donc il suffit de montrer que l'ensemble $\text{Hom}_{\text{an}}(A, L)$ est de cardinal $\leq [E:K]$. Par le lemme de Dedekind (Thm 4) appliqué au monôme $G = (A; \cdot)$, il suffit de montrer que

$\text{Hom}_{An}(A, L)$ est contenu dans son ss-espace de dimension $\leq [E:k]$ du L -espace vectoriel $\text{Hom}_{Ens}(A, L)$. Or $\text{Hom}_{An}(A, L)$ est contenu dans le L -espace des morphismes \mathbb{Z} -linéaires

$$\text{Hom}_{\mathbb{Z}}(A, L) \simeq \text{Hom}_{\mathbb{Z}}(\mathbb{Z}^{[E:k]}, L) \simeq L^{[E:k]}$$

Rque: Supposons \bar{P} séparable. Le groupe $\text{Gal}(L/\mathbb{F}_p)$ agit à gauche sur $\text{Hom}_{An}(A, L)$ par

$$g \cdot \varphi = g \circ \varphi.$$



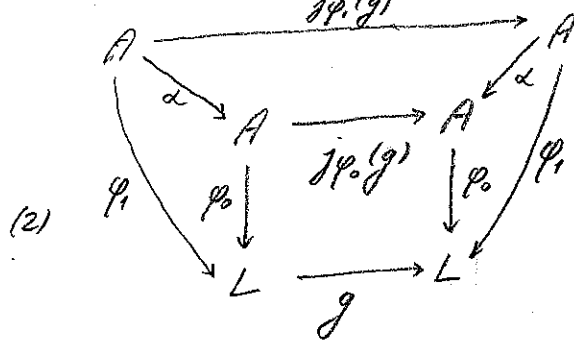
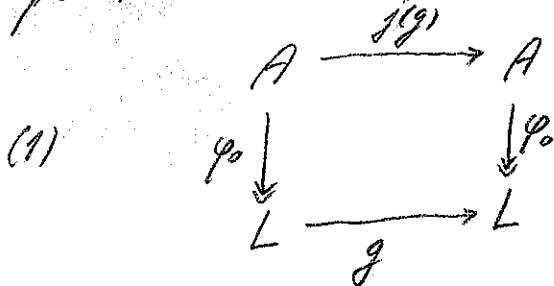
Comme tout φ est surjectif, cette action est libre.

Si on choisit $\varphi_0 \in \text{Hom}_{An}(A, L)$, on obtient donc une injection

$$\text{Gal}(L/\mathbb{F}_p) \hookrightarrow \text{Hom}_{An}(A, L) \xleftarrow{\sim} \text{Gal}(E/\mathbb{Q}).$$

$j = j\varphi_0$

Pour tout $g \in \text{Gal}(L/\mathbb{F}_p)$, $j(g)$ est l'unique autom. de $E \supseteq \mathbb{Q}$ tel que le carré (1)



commute. On en déduit facilement que

$$j: \text{Gal}(L/\mathbb{F}_p) \hookrightarrow \text{Gal}(E/\mathbb{Q})$$

est un morphisme de groupes. Si $\varphi_1: A \rightarrow L$ est un autre morph. d'anneau, on a $\varphi_1 = \varphi_0 \alpha$ pour un unique $\alpha \in \text{Gal}(E/\mathbb{Q})$ et donc

$$j\varphi_1(g) = \alpha^{-1} j\varphi_0(g) \alpha, \quad \forall g \in \text{Gal}(L/\mathbb{F}_p), \text{ voir (2).}$$

Donc $j = j\varphi_0$ est indépendant du choix de φ_0 à conjugaison près.

Finalement, si $\Omega \subset A$ est l'ens. des racines de P et $\bar{\Omega} \subset L$ l'ens. des racines de \bar{P} , alors φ_0 induit une bijection $\Omega \xrightarrow{\sim} \bar{\Omega}$ (voir la d'ém. de la Prop 5) et g et $j(g)$ laissent les ens. de racines stables. D'où des diag. compatibles:

$$\begin{array}{ccc}
 A & \xrightarrow{j(g)} & A \\
 \varphi_0 \downarrow & & \downarrow \varphi_0 \\
 L & \xrightarrow{g} & L
 \end{array}
 \qquad
 \begin{array}{ccc}
 \Omega & \xrightarrow{j(g)} & \Omega \\
 \varphi_0 \downarrow & & \downarrow \varphi_0 \\
 \bar{\Omega} & \xrightarrow{g} & \bar{\Omega}
 \end{array}$$

Ceci achève la démonstration du Thém 6.

Rque: Donné à chaque nombre premier p t.q. \bar{P} est séparable, on a associé une classe de conjugaison

$$C_p = \text{classe de conj. de } j(\mathbb{F}_p)$$

dans $G = \text{Gal}_{\mathbb{Q}}(P)$.

Question: Est-ce que toute classe est atteinte? Et combien de fois?

Réponse: Toute classe est atteinte une infinité de fois.
Plus précisément, on a le théorème remarquable:

Thm 7 (Tchebotareff, 1922): Pour chaque classe de conjugaison C de G ,
(admis) la densité

$$\lim_{n \rightarrow \infty} \frac{|\{p \text{ premier t.q. } \text{disc}(P) < p \leq n \text{ et } C_p = C\}|}{|\{p \text{ premier t.q. } p \leq n\}|}$$
 existe et vaut $|C|/|G|$.

Exemples: 1) On a $C_p = \{e\}$ ssi F_p est l'identité sur \bar{P} se surde dans \mathbb{F}_p . Par le théorème, cela arrive avec "probabilité" $1/|G|$.

2) Pour $P = X^4 - X - 1$, on a $\text{Gal}_{\mathbb{Q}}(P) \cong G_4$. Donc les densités des p t.q. \bar{P} se décompose en des facteurs irréductibles des degrés donnés sont:

décompos.	4	1, 3	2, 2	1, 1, 2	1, 1, 1, 1
densité	1/4	1/3	1/8	1/4	1/24

* Жуковскій Троицкскій Уездомрътвѣ, 1894 (Kamenets-Podolsk) - 1947 (Kiev)

III Introduction à la géométrie algébrique

1. Un peu d'algèbre commutative

Convention : anneau = anneau commutatif avec 1
morphisme d'anneau = morph. compatible avec la multiplication et qui préserve 1.

Exemple : $A \rightarrow A \times A, a \mapsto (a, 0)$ est un morphisme d'anneaux
ssi $A = 0$.

1.1 Radical de Jacobson, racine d'un idéal, nilradical

Soit A un anneau non nul.

Def : Le radical de Jacobson de A est l'ensemble
 $\text{Rad}A := \{x \in A \mid 1 + ax \text{ est inversible pour tout } a \in A\}$.

Lemme 1 : a) $\text{Rad}A$ est un idéal de A . On a $1 + \text{Rad}A \subseteq A^*$
et $\text{Rad}A$ est le plus grand idéal avec cette propriété.
b) $\text{Rad}A$ est l'intersection des idéaux maximaux de A .

Dém. : a) Pour $x \in \text{Rad}A$ et $a \in A$, on a $ax \in \text{Rad}A$, par définition.

Soient $x, y \in \text{Rad}A$. On a

$$1 + (x+y) = (1+x) + y \text{ et donc } (1+x)^{-1}(1+x+y) = 1 + (1+x)^{-1}y$$

ce qui montre que $1+x+y$ est inversible. Donc $\text{Rad}A$ est un idéal.

Le reste est clair.

b) Montrons que le complémentaire de $\text{Rad}A$ est égal au complémentaire de l'intersection des idéaux maximaux :

$$y \notin \text{Rad}A \Rightarrow \exists a \in A \text{ t.q. } 1+ay \notin A^* \Rightarrow A \cdot (1+ay) \neq A$$

$$\Rightarrow \exists m \text{ idéal max. t.q. } (1+ay) \cdot A \subseteq m$$

$$\Rightarrow 1+ay \in m \Rightarrow y \notin m \text{ (sinon, on aurait } 1 \in m).$$

$$y \notin \bigcap_{m \text{ max.}} m \Rightarrow \exists m_0 \text{ max. t.q. } y \notin m_0.$$

$$\Rightarrow \exists a \text{ t.q. } 1+ay \in m_0 \text{ (car } A/m_0 \text{ est un corps)}$$

$$\Rightarrow 1+ay \text{ n'est pas inversible}$$

$$\Rightarrow y \notin \text{Rad} A. \quad \checkmark$$

Def: Soit I un idéal de A . La racine de I (= "radical" de I) est l'ensemble

$$\sqrt{I} = \{ a \in A \mid \exists n \geq 1 \text{ t.q. } a^n \in I \}$$

L'idéal I est radical si $I = \sqrt{I}$.

Lemme 2: a) \sqrt{I} est un idéal. C'est le plus petit idéal radical contenant I . Tout idéal premier est radical.

b) On a $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ pour tout idéal J .

c) \sqrt{I} est l'intersection des idéaux premiers contenant I .

Dém.: a) Clairement si $x \in I$ et $a \in A$, alors $ax \in I$. Soient $x, y \in \sqrt{I}$

et $n, m \geq 1$ t.q. $x^n \in I$ et $y^m \in I$. Alors

$$(x+y)^{n+m} = \sum_{p+q=n+m} \binom{n+m}{p} x^p y^q \in I$$

$\underbrace{\hspace{10em}}_{\in I \text{ car } p \geq n \text{ ou } q \geq m.}$

Si $x \in \sqrt{I}$, alors $x^n \in I$ et $(x^n)^m \in I$ pour des $n, m \geq 1$.

Donc $x \in \sqrt{I}$ et on a $\sqrt{I} = \sqrt{I}$. Si $J \supseteq I$ est radical et $x^n \in I$, alors $x^n \in J$, donc $x \in J$. Donc $J \supseteq \sqrt{I}$. Si p est

premier et $x^n \in p$, alors $x^n = 0$ dans A/p , qui est intègre.

Donc $x = 0$ dans A/p et $x \in p$. b) Exercice!

c) Montrons que le complémentaire de \sqrt{I} est égal au complémentaire de l'intersection des idéaux premiers contenant I . Si x n'est pas dans l'intersection, alors $x \notin p$ pour un premier p contenant I . Donc $x^n \notin p$, $\forall n \geq 1$, et $x \notin \sqrt{I}$. Réciproquement, supposons que $x \notin \sqrt{I}$. Alors $x^n \notin I$, $\forall n \geq 1$. Considérons l'ens. ordonné E des idéaux J contenant I t.q. $x^n \notin J$, $\forall n \geq 1$. Alors E est non vide (car $I \in E$) et toute famille non vide d'éléments de E admet une borne supérieure (la réunion). Soit J_0 maximal dans E (Zorn). Montrons que J_0 est premier. Soient $a, b \in A$ t.q. $a \notin J_0$ et $b \notin J_0$. Alors il existe $n, m \geq 1$ t.q. $x^n \in (a) + J_0$ et $x^m \in (b) + J_0$, par la maximalité de J_0 . Donc $x^{n+m} \in (ab) + J_0$ et $ab \notin J_0$ car $x^{n+m} \notin J_0$. On a montré que $x \notin \sqrt{I}$ implique que $x \notin J_0$ pour l'idéal premier J_0 . \checkmark

Proposition 3: Soit $S \subseteq A$ une partie multiplicative, i.e. $1 \in S$ et $SS \subseteq S$.

Si J_0 est maximal dans l'ens. ordonné des idéaux qui ne rencontrent pas S , alors J_0 est premier.

Déf: Le nilradical de A est l'ensemble des éléments nilpotents de A .

Rem: le nilradical est donc égal à $\sqrt{(0)}$ et on a

$$\sqrt{(0)} = \bigcap_{p \text{ premier}} p$$

par le lemme 2. Notons que $\sqrt{(0)} \subseteq \text{Rad} A$.