Séminaire Claude Chevalley

A. Grothendieck

Sous-groupes de Cartan, éléments réguliers. Groupes algébriques affines de dimension 1

Séminaire Claude Chevalley, tome 1 (1956-1958), exp. n° 7, p. 1-9

<http://www.numdam.org/item?id=SCC_1956-1958__1__A7_0>

Séminaire C. CHEVALLEY
E.N.S., 1956/57
Exposé n° 7

-:-:-:-

SOUS-GROUPES DE CARTAN, ÉLÉMENTS RÉGULIERS. GROUPES ALGÉBRIQUES AFFINES DE DIMENSION 1.

(Exposé de A. GROTHENDIECK, le 14.1.1957)

1.- SOUS-GROUPES DE CARTAN.

La définition qui suit, valable pour tout "groupe abstrait", est due à Chevalley :

DÉFINITION 1.- Soit G un groupe, on appelle sous-groupe de Cartan de G tout sous-groupe nilpotent maximal dont tout sous-groupe d'indice fini est d'indice fini dans son normalisateur.

Dans le cas où G est un groupe algébrique, un sous-groupe de Cartan C est nécessairement fermé (puisque l'adhérence d'un groupe nilpotent est nilpotent, cf. exposé 3) ; d'autre part, si C est un sous-groupe fermé de G, les conditions "tout sous-groupe d'indice fini dans C est d'indice fini dans son normalisateur" équivaut à "C_o est d'indice fini dans son normalisateur". En effet, la première implique trivialement la seconde, supposons inversement la seconde vérifiée, soit H un sous-groupe d'indice fini dans C, alors $\overline{H}$ est compris entre C_o et C, et admet donc C_o comme composante connexe de l'élément neutre ; donc le normalisateur de H, évidemment contenu dans celui de $\overline{H}$, est contenu dans celui de C_o, d'où résulte que $H \cap C_o$ est d'indice fini dans $N(H)$, et à fortiori H est d'indice fini dans $N(H)$.

THÉORÈME 1.- Soit G un groupe algébrique affine connexe, C un sous-groupe de G, les conditions suivantes sont équivalentes : (i) C est un sous-groupe de Cartan (ii) C est le centralisateur d'un tore maximal (iii) C est nilpotent et identique à son normalisateur connexe.

En particulier, compte tenu du théorème de conjugaison (exposé 6, théorème 4, c)) :

COROLLAIRE.- Les sous-groupes de Cartan de G sont connexes et conjugués entre eux.

DÉMONSTRATION DU THÉORÈME 1.- Admettons un instant (iii) $\Longrightarrow$ (ii), prouvons (ii) $\Longrightarrow$ (i) et (i) $\Longrightarrow$ (iii). Soit C le centralisateur d'un tore maximal, nous savons que C est nilpotent maximal et identique à son normalisateur connexe (exposé 6, théorème 6 c)), à fortiori il est d'indice fini dans son normalisateur, donc C est un sous-groupe de Cartan d'après ce qui a été dit plus haut. Supposons que C soit un sous-groupe de Cartan, alors C est nilpotent et C_o est d'indice fini dans son normalisateur, donc d'après (iii) $\Longrightarrow$ (ii), C_o est le centralisateur d'un tore maximal, donc un sous-groupe de Cartan et par suite nilpotent maximal, d'où $C = C_o$, et C est bien le centralisateur d'un tore maximal. Reste donc à prouver (iii) $\Longrightarrow$ (ii). Soit donc C un sous-groupe nilpotent de G identique à son normalisateur connexe ; prouvons que c'est le centralisateur d'un tore maximal. Soit B un sous-groupe de Borel de G contenant C ; C est un sous-groupe nilpotent de B identique à son normalisateur connexe dans B ; il suffit de prouver qu'il est le centralisateur dans B d'un tore maximal de B (car en vertu de l'exposé 6, théorème 6 d) et théorème 4 c), c'est alors aussi le centralisateur d'un tore maximal de G). On est donc ramené au cas où G est résoluble. En vertu de l'exposé 6, théorème 2 et théorème 3, on a $C = S \times C_u$ où $S = C_s$ est l'unique tore maximal de C, et si T désigne un tore maximal de G contenant S, on a $G = T.G_u$ (produit semi-direct). Soit M le centralisateur connexe de S, M contient T et est donc de la forme $T.M_u$ (exposé 6, théorème 3), où évidemment $M_u \supset C_u$; je dis qu'en fait $M_u = C_u$. Pour ceci admettons un instant le :

LEMME.- Soit M un groupe affine nilpotent connexe, N un sous-groupe connexe de M distinct de M, alors N est distinct de son normalisateur connexe.

Si on avait $M_u \neq C_u$, le normalisateur connexe N de C_u dans M_u serait donc $\neq C_u$, et alors SxN serait un groupe connexe non contenu dans C normalisant C, contrairement à l'hypothèse sur C. Ainsi $C_u = M_u$; or M_u est évidemment normalisé par T (puisque T commute à S), donc C est normalisé par T et par suite $T \subset C$, d'où $S = T$, donc $C = S \cdot C_u = T.M_u$ est bien le centralisateur connexe (= le centralisateur) du tore maximal T. Reste à démontrer le lemme. On procède par récurrence sur dim.M, le cas où dim.M=0 étant clair. Soit dim.M=n > 0 ; si N ne contient pas la composante connexe H de l'élément neutre dans le centre de M, le lemme est clair, autrement on applique l'hypothèse de récurrence à M/H

(qui est de dimension $< n$) et au sous-groupe N/H .

2.- ÉLÉMENTS RÉGULIERS.

DÉFINITION 2.- Soit G un groupe. Un élément de G est dit régulier s'il est contenu dans un sous-groupe de Cartan et un seul de G .

THEOREME 2.- Soient G un groupe algébrique affine connexe, g un élément de G . Les conditions suivantes sur g sont équivalentes : (i) g est régulier i.e. (définition 2) g est contenu dans un sous-groupe de Cartan et un seul (i bis) l'ensemble des sous-groupes de Cartan contenant g est fini non vide (ii) g_s est contenu dans un seul tore maximal (iii) le normalisateur de g_s est de dimension minimum (iv). Le centralisateur connexe de g_s est un sous-groupe de Cartan (v). Le centralisateur connexe de g_s est nilpotent.

Soit T un tore maximal contenant g_s (il en existe, exposé 6, théorème 5 c)) C son centralisateur (C est connexe, nilpotent, et c'est un sous-groupe de Cartan, d'après le théorème 1) ; C est contenu dans le centralisateur connexe $Z(g_s)_o$ de g_s . Comme il existe des éléments s de T tels que tout $x \in G$ satisfaisant à $xsx^{-1} \in T$ normalise C (cf. exposé 6, démonstration du théorème 5 a)), et que $C = N(T)_o$, il existe des éléments dans T dont le centralisateur connexe est réduit à C . Donc la dimension minimum envisagée dans (iii) est celle de C , et (iii) équivaut à $Z(g_s)_o = C$, donc à (iv) et à (v) (car un sous-groupe contenant un sous-groupe de Cartan C est un sous-groupe de Cartan si et seulement si il est identique à C , ou encore si et seulement si il est nilpotent !). D'ailleurs, les tores maximaux contenant g_s sont évidemment les tores maximaux de $Z(g_s)_o$, donc (ii) signifie que $Z(g_s)_o$ a un seul tore maximal, ce qui équivaut à (v) en vertu de l'exposé 6, théorème 4, corollaire 2. Ainsi les conditions (ii) , (iii) , (iv) et (v) sont équivalentes, elles impliquent de plus (i) , car d'une part g appartient à $Z(g_s)_o$ (exposé 6, théorème 6, corollaire 2, démontré tout exprès pour ça) donc à un sous-groupe de Cartan, d'autre part si g appartient à un sous-groupe de Cartan C , C est le centralisateur d'un tore maximal T en vertu du théorème 1, et comme $T = C_s$ on aura $g_s \in T$, donc T et par suite C est uniquement déterminé. Comme (i) implique (i bis) trivialement, il reste à prouver que (i bis) implique que $Z(g_s)_o$ n'a qu'un seul tore maximal. Soit C

un groupe de Cartan contenant g ; alors $g \in C \subset Z(g_s)_o$, et, comme $Z(g_s)_o$ contient un sous-groupe de Cartan C , les sous-groupes de Cartan de $Z(g_s)_o$ sont des sous-groupes de Cartan de G , ce qui nous ramène au cas où $G = Z(g_s)_o$, i.e. au cas où g_s est dans le centre Z de G . Il est immédiat sur la définition 1 que les sous-groupes de Cartan de G sont les images réciproques des sous-groupes de Cartan de G/Z , donc l'image de g dans G/Z est un élément unipotent satisfaisant (i bis) , ce qui nous ramène à montrer ceci : si G est un groupe algébrique affine connexe ayant un élément unipotent $u = g$ satisfaisant (i bis) , G est nilpotent. Comme u est contenu dans un sous-groupe de Borel de G (exposé 6, théorème 5, b)) , et que les sous-groupes de Cartan de B sont des sous-groupes de Cartan de G (exposé 6, théorème 6, d)) u satisfait (i bis) dans B ; prouvons que B est nilpotent, il s'ensuivra que G l'est (exposé 6, théorème 4, corollaire 2). Cela nous ramène au cas où G est résoluble. Soit $C = TxC_u$ un sous-groupe de Cartan de G contenant u , nous voulons montrer $C_u = G_u$ (ce qui prouvera que G est nilpotent). Dans le cas contraire, en vertu du lemme du n° 1 appliqué aux groupes nilpotents connexes G_u et C_u , le normalisateur connexe L de C_u dans G_u serait $\neq C_u$, et, comme $L \cap N(C) = C_u$, les vCv^{-1} pour $v \in L$ forment une infinité de sous-groupes de Cartan de G contenant u , contrairement à l'hypothèse. C.Q.F.D.

COROLLAIRE 1.- Pour que g soit régulier, il faut et il suffit que g_s le soit.

COROLLAIRE 2.- Soit G un groupe algébrique affine connexe. L'ensemble des points réguliers de G est un ensemble ouvert dense dans G .

Cette assertion résulte aussitôt de l'équivalence de (i) et (i bis), de l'existence d'éléments réguliers (visible sur la condition (iii)) et du corollaire au lemme 5 de l'exposé 6, n° 5 , compte tenu de ce que $e = 0$ puisque $N(C)_o = C$.

REMARQUE.- Soit m le nombre de sous-groupes de Borel de G contenant un sous-groupe de Cartan C , (on verra plus tard que m est l'ordre du groupe de Weyl $N(C)/C$, mais dès maintenant il résulte facilement du théorème de conjugaison que les sous-groupes de Borel contenant C sont conjugués par des opérations du groupe de Weyl, en particulier il n'y en a qu'un nombre fini). Soit g un élément régulier de G , C l'unique groupe de Cartan

le contenant ; alors les sous-groupes de Borel B contenant g sont exactement ceux contenant C (et il y en a donc exactement m) . En effet, si B contient g , il contient g_s , donc l'unique tore maximal T de G contenant g_s , donc aussi C = C(T) en vertu de l'exposé 6, théorème 6 d). Dans le cas où G est semi-simple, on peut montrer la réciproque, du moins si g est semi-simple (condition d'ailleurs nécessaire, dans ce cas, pour que g soit régulier, comme nous verrons plus tard) : si g est contenu dans exactement m sous-groupes de Borel, et est semi-simple, il est régulier. (Résulte facilement du fait qu'un tore maximal est alors l'intersection des sous-groupes de Borel de G qui le contiennent).

3.- THÉORÈMES DE CONSERVATION.

THÉORÈME 3.- a) Soit f une représentation linéaire rationnelle d'un groupe algébrique affine connexe G sur un autre G' . Alors les sous-groupes de Borel (resp. les tores maximaux, resp. les sous-groupes de Cartan) de G' sont les images par f des sous-groupes de Borel (resp. ...) de G ,

b) L'application f transforme éléments réguliers en éléments réguliers.

c), Soit H un sous-groupe connexe invariant de G , alors les sous-groupes de Borel (resp. les tores maximaux) de H sont les composantes connexes de l'élément neutre des intersections avec H de certains sous-groupes de Borel (resp. tores maximaux) de G .

La dernière assertion est triviale, car un sous-groupe de Borel (resp. un tore maximal) de H est contenu dans un sous-groupe de Borel (resp. un tore maximal) de G , donc contenu dans la composante connexe de l'intersection de ce dernier avec H , donc identique à cette intersection en vertu de son caractère maximal. Pour la première assertion, il suffit de prouver que f transforme un sous-groupe de Borel (resp. ...) en un sous-groupe de Borel (resp. ...) , les théorèmes de conjugaison impliquent alors qu'on obtient ainsi tous les sous-goupes de Borel (resp. ...) de G' . Soit B un sous-groupe de Borel de G , posons B' = f(B) , on a une application régulière surjective $G/B \longrightarrow G'/B'$, comme G/B est complète (exposé 6, théorème 4 b)) il en est de même de G'/B' , donc B' contient un sous-groupe de Borel de G' (loc. cité), et étant lui-même résoluble et connexe est un sous-groupe de Borel. Soit T un tore maximal de G , B un sous-groupe de Borel de G contenant T , posons T' = f(T) , B' = f(B) , pour prouver

que T' est un tore maximal de G' il suffit de prouver que c'est un tore maximal du sous-groupe de Borel B', ce qui nous ramène au cas G résoluble. Mais alors on a $G = T.G_u$ (exposé 6, théorème 3) d'où $f(G) = f(T).f(G_u)$, ce qui prouve que $f(T)$ est un tore maximal du groupe résoluble $G' = f(G)$. Soit enfin C le centralisateur de T dans G, prouvons que son image C' est le centralisateur de T' dans G' ; utilisant l'exposé 6, théorème 6, d) on est encore ramené au cas où $G = B$, $G' = B'$, i.e. où G est résoluble. Il faut montrer que si g est tel que $f(g)$ centralise $f(T)$, alors $f(g) \in f(C)$. L'hypothèse signifie que $gTg^{-1} \subset H$, où $H = f^{-1}(T')_o$; en vertu du théorème de conjugaison appliqué aux deux tores maximaux T, gTg^{-1} de H, il existe $h \in H$ tel que $hTh^{-1} = gTg^{-1}$ i.e. tel que $g^{-1}h = x$ normalise T, donc soit dans C (exposé 6, théorème 1, corollaire 3), d'où résulte aussitôt que $f(g) = f(h)f(x)^{-1}$ est dans $f(C)$.

Soit g un élément régulier de G, montrons que $g' = f(g)$ est régulier. Comme $f(g)_s = f(g)_s$ et qu'un élément est régulier si et seulement si sa partie semi-simple l'est (théorème 2), on peut supposer g semi-simple. Soit N le noyau de f, l'application f se factorise en $G \to G/N_o \to G'$, ce qui nous ramène à envisager séparément les cas où N est connexe, et celui où N est fini.

a) N est connexe. Soit S un tore maximal de G' contenant g' (exposé 6, théorème 5 c)), soit $H = f^{-1}(S)$, c'est un groupe affine connexe, d'après la première partie du théorème 3 il contient un tore maximal de G s'appliquant sur S, donc par conjugaison tous les tores maximaux de H sont maximaux dans G et s'appliquent sur S. On sait que l'un d'eux contient l'élément semi-simple g (loc. cité) ; or g étant régulier est contenu dans un unique tore maximal T, comme $S = f(T)$ il n'y a qu'un seul tore maximal de G' contenant g', i.e. g' est régulier dans G' (théorème 2).

b) N est fini. Alors, G étant connexe, N est nécessairement dans le centre de G, donc les sous-groupes de Cartan de G sont les images réciproques des sous-groupes de Cartan de G', et la conclusion résulte aussitôt de la définition des éléments réguliers.

4.- GROUPES AFFINES DE DIMENSION 1.

THÉORÈME 4.- Soit G un groupe algébrique affine connexe de dimension 1, alors G est isomorphe à k ou à k^*.

Supposons que G ne soit pas isomorphe à $\underline{k}^*$. Alors pour des raisons de dimension, un tore maximal de G est réduit à l'élément neutre, donc (théorème 4) G est nilpotent et $G = G_u$. Comme le groupe des commutateurs de G est connexe et $\neq G$, il est réduit à 0, donc G est abélien unipotent. D'après la démonstration de l'exposé 6, théorème 1, corollaire 1, G admet une représentation rationnelle non triviale dans $\underline{k}$ ou $\underline{k}^*$, comme G est unipotent c'est donc une représentation f de G dans $\underline{k}$, de noyau N fini puisque G est de dimension 1 et $f \neq 0$. Si la caractéristique est nulle, le groupe fermé engendré par $g \in G$, $g \neq 0$ est isomorphe à $\underline{k}$ (exposé 4, proposition 4), donc G est isomorphe à $\underline{k}$, on peut donc supposer la caractéristique $p \neq 0$. Alors le noyau N de f est un p-groupe (loc. cité, compte tenu que $G = G_u$).

Nous allons prouver que G/N est isomorphe à $\underline{k}$, puis en conclure que G est isomorphe à $\underline{k}$ par récurrence sur l'entier n tel que N soit d'ordre p^n, ce qui nous ramène à prouver les deux lemmes suivants :

LEMME 2.- Soit G un groupe algébrique connexe affine admettant une représentation rationnelle bijective x dans le groupe $\underline{k}$, alors G est isomorphe à $\underline{k}$. (Mais en général x n'est pas un isomorphisme !)

LEMME 3.- Soit G un groupe algébrique affine connexe abélien unipotent admettant un sous-groupe N d'ordre p tel que G/N soit isomorphe à $\underline{k}$ Alors H est isomorphe à $\underline{k}$.

DÉMONSTRATION DU LEMME 2.- En vertu de l'exposé 5, théorème 1, corollaire 4, le corps $k(G)$ des fonctions rationnelles sur G est une extension algébrique finie purement inséparable du corps des fonctions rationnelles sur $G' = \underline{k}$, qui s'identifie à l'extension transcendante pure $\underline{k}(x)$ de $\underline{k}$ engendrée par l'élément x de $\underline{k}(G)$. Ainsi $\underline{k}(G)$ est une extension radicielle de $\underline{k}(x)$, son degré sur $\underline{k}(x)$ est de la forme p^n, or il est bien connu que, $\underline{k}$ étant un corps algébriquement clos, il existe à un isomorphisme près une extension radicielle K et une seule de degré p^n de $\underline{k}(x)$, savoir $\underline{k}(x)^{p^{-n}} = \underline{k}(x^{p^{-n}})$. (Pour le voir, une récurrence immédiate nous ramène au cas où $n = 1$, mais alors $\underline{k}(x) \subset K \subset \underline{k}(x)^{p^{-1}}$, et comme $\underline{k}(x)^{p^{-1}}$ est de degré p sur $\underline{k}(x)$, car $\underline{k}(x)$ est de degré p sur $\underline{k}(x)^p = \underline{k}(x^p)$, on a nécessairement $K = k(x)^{p^{-1}}$. Ainsi $x^{p^{-n}}$ est un générateur de $\underline{k}(G)$

sur $\underline{k}$, or x étant une fonction régulière sur G il en est de même de $x^{p^{-n}}$ (puisque G est normal), qui est donc une représentation rationnelle de G dans $G' = \underline{k}$, bijective et birationnelle. Comme G' est normale, c'est donc en vertu du Main Theorem (exposé 5, théorème 2) un isomorphisme de variétés algébriques, donc un isomorphisme de groupes algébriques.

DÉMONSTRATION DU LEMME 3.- Soit x un isomorphisme de G/N sur $\underline{k}$, alors $\underline{k}(G/N)$ s'identifie à $K = \underline{k}(x)$, et $L = \underline{k}(G)$ en est une extension galoisienne de groupe de Galois N , (de façon générale, si un groupe fini N opère dans une variété G , de telle façon que toute orbite de N soit contenue dans un ouvert affine, il est facile de définir la variété quotient G/N , par la condition que sa topologie soit la topologie quotient, et que les fonctions régulières sur un ouvert soient les fonctions régulières invariantes sous G sur l'ouvert image réciproque. Et on prouve aisément que les fonctions rationnelles sur G/N s'identifient alors aux fonctions rationnelles sur G invariantes par N , de sorte que $\underline{k}(G)$ est une extension galoisienne de $\underline{k}(G)$, ayant N pour groupe de Galois). Ici N est isomorphe à $Z/(p) = \underline{Z}_p$ une fois choisi un générateur σ de N . En vertu de la théorie de Galois des extensions galoisiennes de degré p ("extensions d'Artin-Schreier"), une telle extension L de K s'obtient en adjoignant à K une racine d'une équation de la forme $X^p - X = u$, où u est un élément de K tel que cette équation soit irréductible, i.e. non de la forme $v^p - v$ $(v \in K)$. Ceci résulte de $Tr_{L/K} 1 = p.1 = 0$, qui implique en vertu d'un théorème bien connu de Hilbert qu'on peut trouver $f \in L$ telle que $\sigma(f) - f = 1$, et posant alors $u = f^p - f$, on aura $u \in K$) . D'ailleurs, l'extension L ne change pas si on remplace u par $u + u'$, où u' est de la forme $v^p - v$ $(v \in K)$. Dans le cas actuel, le groupe N opérant sans points fixes dans G , G/N est non ramifié dans L (exposé 5). On en conclut facilement qu'on peut choisir u fonction régulière sur G/N , soit directement en utilisant le fait que $G/N = \underline{k}$, et la décomposition canonique des fonctions rationnelles en "éléments simples" ; soit mieux en invoquant la suite exacte générale, donnant le groupe $H_1(X , \underline{Z}_p)$ des revêtements non ramifiés (irréductibles ou non) d'une variété normale X , à l'aide du groupe $H^0(X , \underline{O})$ des fonctions régulières sur X , du groupe $H^1(X , \underline{O})$ ($\underline{O}$ désigne le faisceau des anneaux locaux sur X), et de l'opération déduite de l'endomorphisme $f \to f^p - f$ du faisceau $\underline{O}$:

$$0 \to Z_p \to H^0(X , \underline{0}) \to H^0(X , \underline{0}) \to H^1(X , Z_p) \to H^1(X , \underline{0}) \to H^1(X , \underline{0})$$

(cette suite exacte s'établit élémentairement à l'aide de la théorie de Artin-Schreier, et du critère de non-ramification par le discriminant, donnée dans l'exposé 5). Dans le cas actuel, $X = G/N = \underline{k}$ est une variété affine, donc $H^1(X , \underline{0}) = 0$ ce qui implique bien qu'on peut prendre $u \in H^0(X , \underline{0})$. Utilisons le fait que G est un groupe ; le diagramme

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ \downarrow & & \downarrow \\ X \times X & \xrightarrow{h} & X \end{array}$$

(où $X = G/N$, les morphismes horizontaux étant donnés par les lois de groupe) définit un homomorphisme du revêtement produit GxG de XxX dans le revêtement image réciproque du revêtement G par h , compatible avec l'homomorphisme $\underline{Z}_p \times \underline{Z}_p \to \underline{Z}_p$ des groupes structuraux. Si D est le noyau de ce dernier homomorphisme, on en conclut un isomorphisme du revêtement GxG/D de XxX sur le revêtement $h^{-1}(G)$. Or ces revêtements sont définis respectivement par les fonctions $u(x) + u(y)$ et $u(h(x , y)) = u(x + y)$ sur XxX , comme le montre un calcul immédiat. On a donc :

$$(*) \qquad u(x + y) - u(x) - u(y) = w(x , y)^p - w(x , y)$$

où w est une fonction régulière sur XxX . Supposons maintenant que u , qui est un polynôme en x , soit choisi de façon que son degré n soit minimum, évidemment on a $n \geqslant 1$, prouvons $n = 1$. Tout d'abord n n'est pas multiple de p , car si le terme dominant de u était ax^{mp} , on pourrait remplacer u par $u' = u - ((bx^m)^p - bx^m)$, où $b \in \underline{k}$ est tel que $b^p = a$, et on aurait $\deg.u' < \deg.u$. Si on avait $n \neq 1$, le premier membre de (*) serait un polynôme de degré n exactement, tandis que le deuxième membre est de degré multiple de p , ce qui est absurde. On a donc $u = ax + b$, et on peut le remplacer par $u = ax$. Ainsi, $\underline{k}(G)$ est engendré sur $\underline{k}(x)$ par une fonction régulière f telle que $f^p - f = ax$, il en résulte qu'on a en fait $\underline{k}(G) = \underline{k}(f)$. Je dis que f est un homomorphisme de groupes, i.e. qu'on a $f(g + g') - f(g) - f(g') = 0$ pour $g , g' \in G$. En effet, si le premier membre est noté $F(g , g')$, on aura $F(g , g')^p - F(g , g') = ax(g + g') - ax(g) - ax(g') = 0$ puisque x est un homomorphisme de groupes, cela prouve que $F(g , g')$ prend ses valeurs dans le groupe à p éléments engendré par $1 \in \underline{k}$, donc est constante ($G \times G$ étant connexe) , donc nulle comme on voit en faisant $g = g' = 0$. Ainsi f est un homomorphisme régulier et birationnel de G dans $\underline{k}$, donc un isomorphisme en vertu du Main Theorem.