ON ALGEBRAIC GROUPS AND HOMOGENEOUS SPACES *

By ANDRÉ WEIL.

In a recent paper in the same JOURNAL ([4] of the bibliography; quoted hereafter as AG), I gave some results on algebraic groups and transformation-spaces, which supplement those in my *Variétés abéliennes* ([3]; quoted as VA). Applications will now be made of that theory to somewhat more specific questions. In no. 1, a rather general procedure is described for obtaining, from a given transformation-space S with respect to a group G and from a suitable cycle on S, another transformation-space with respect to the same group. As shown in no. 2, this includes as a special case the construction of coset-spaces and of factor-groups; thanks to the main theorem in AG, these can now be defined without enlarging the groundfield, whereas such an enlargement was required in their construction as previously given by S. Nakano ([2]); except for this, we have substantially followed his method.

The rest of this paper is chiefly devoted to "principal homogeneous spaces," i.e. to those homogeneous spaces on which the group operates in a simply transitive manner. The pair consisting of such a space and of one point on it does not differ materially from a group; thus there is little incentive for studying those spaces as long as one is not paying any attention to the groundfield or if the groundfield is algebraically closed. But it can happen that a principal homogeneous space contains no rational point over the groundfield over which it is defined; an example of this is given by the plane curve $X^3 + pY^3 = p^2$ over the rational number-field, where p is a rational prime; this may be considered as a principal homogeneous space with respect to its jacobian variety, which is the plane curve $Y^2 = 4X^3 - 27$. More generally, Chow's work (cf. [1]) has shown that it is not always possible to map a curve "canonically" into its jacobian variety by a mapping defined over the groundfield, but that the curve can always be so mapped into a suitable principal homogeneous space with respect to its jacobian variety. This, among other results, will be proved again here by a different method, which can be extended at once to a variety V of higher dimension and to its Albanese variety, provided the groundfield is one over which the latter is defined. It will also be shown that the classes of principal homogeneous

* Received December 27, 1954.

spaces with respect to a commutative group can be arranged into a torsion-group, i.e. a group whose elements are all of finite order; and it follows at once from the results of no. 5 that this group must be countable if the groundfield is finitely generated over the prime field. There seems to be no reason why it should be finite, even if the groundfield is the field of rational numbers; a more detailed investigation of its structure, e.g. for the case of an elliptic curve over the field of rational numbers, would be of considerable interest from the point of view of the theory of diophantine equations.

1. Let G be a group and S a transformation-space with respect to G, both defined over a field k. Let Z be either a divisor on S or a cycle on S whose components have coefficients which are prime to the characteristic of the universal domain. We denote by sZ, for any $s \in G$, the transform of Z by the mapping $u \to su$ of S onto itself. Let K be an overfield of k over which Z is rational. Let x be generic over K on G; by Prop. 6 of the Appendix of AG, there is a finitely generated extension $k(t)$ of k which is the smallest overfield of k over which xZ is rational; as xZ is rational over $K(x)$, we have $k(t) \subset K(x)$. If x' is also a generic point of G over K, and σ is the isomorphism of $K(x)$ onto $K(x')$ over K which maps x onto x', σ will transform xZ into $x'Z$; if t' is the image of t under σ, $k(t')$ will then be the smallest overfield of k over which $x'Z$ is rational, and, by Prop. 6 of the Appendix of AG, the cycle $x'Z$ depends only upon t'; in other words, if σ_1 is an isomorphism of $K(x)$ onto a field $K(x_1')$, mapping x onto x_1' and t onto t_1', we have $x'Z = x_1'Z$ if and only if $t' = t_1'$. In particular, take $x' = yx$, with y generic over $K(x)$ on G; then $k(t')$ is the smallest overfield of k over which yxZ is rational; as yxZ can be written as $y(xZ)$, it is rational over $k(y, t)$, so that $k(t') \subset k(y, t)$; similarly, xZ can be written as $y^{-1}(yxZ)$ and is therefore rational over $k(y, t')$, so that $k(t) \subset k(y, t')$. This shows that $k(y, t) = k(y, t')$.

Put now $z = yx$, so that we have $k(t') \subset K(z)$; take y' generic over $K(x, y)$ on G, and call τ the isomorphism of $K(z)$ onto $K(y'z)$ over K which maps z onto $y'z = y'yx$; let t'' be the image of t' under τ. Then t'' is the image of t under the isomorphism $\tau \circ \sigma$ of $K(x)$ onto $K(y'yx)$ over K which maps x onto $y'yx$.

If Z is such that $k(t)$ is a regular extension of k, then we may call T the locus of t over k and, with the above notations, we may write $t' = g(y, t)$, where g is a mapping of $G \times T$ into T, defined over k. Then the results we have just proved mean that g satisfies (TG 1, 2) of AG, no. 2, i.e. that it is a normal law between G and T. Applying now the main theorem of AG, we get the following result:

PROPOSITION 1. *Let G be a group and S a transformation-space with respect to G, both defined over a field k. Let Z be either a divisor on S or a cycle on S whose components have coefficients which are prime to the characteristic. Let K be an overfield of k over which Z is rational; and assume that, if x is generic over K on G, the smallest extension k' of k over which xZ is rational is a regular extension of k. Then there is a transformation-space T with respect to G, defined over k, and an everywhere defined mapping F of G into T, defined over K, such that the point $t = F(x)$ is generic over k on T, that $k' = k(t)$, and that $F(ss') = sF(s')$ for all s, s' on G. For any s, s' in G, we have $F(s) = F(s')$ if and only if $sZ = s'Z$. If Z is algebraic over k, one can take for T a homogeneous space with respect to G.*

The existence of a transformation-space T with a generic point t over k such that $k' = k(t)$ has been proved above; moreover, with the same notations as above, we have $k(t) \subset K(x)$, $k(t') \subset K(yx)$, $t' = yt$; as $K(x)$, $K(yx)$ are independent extensions of K, this shows, if K is algebraic over k, that $k(t)$, $k(t')$ are then independent extensions of k, i.e. that T is pre-homogeneous, so that, by the main theorem of AG, we may replace it by a birationally equivalent homogeneous space. As $k(t) \subset K(x)$, we may write $t = F(x)$, with F defined over K; then we have $yt = F(yx)$, i.e. $F(yx) = yF(x)$, for y generic over $K(x)$ on G. This may be written as $F(x) = y^{-1}F(yx)$, which shows, if s is any point of G and y is taken generic over $K(s)$ on G, that F is defined at s. As F is everywhere defined, the relation $F(yx) = yF(x)$ implies $F(ss') = sF(s')$ for all s, s' on G. Now, for any s, s' on G, take x generic over $K(s, s')$ on G; then xs, xs' are both generic over K on G, and therefore, if σ is the isomorphism of $K(xs)$ onto $K(xs')$ over K which maps xs onto xs', σ will map $F(xs)$ onto $F(xs')$ and the cycle xsZ onto $xs'Z$; then, as we have seen above, we have $xsZ = xs'Z$ if and only if $F(xs) = F(xs')$; as the latter relation can be written $xF(s) = xF(s')$, so that these two relations are respectively equivalent to $sZ = s'Z$ and to $F(s) = F(s')$, this completes our proof.

2. We first apply Prop. 1 to the construction of the homogeneous space defined by a group G and a subgroup of G.

PROPOSITION 2. *Let G be a group, defined over a field k; let Z be a rational cycle over k on G, consisting of components with coefficient* 1, *and such that its support $|Z|$ is a subgroup of G. Then there is a homogeneous space H with respect to G, defined over k, and a rational point a over k on H, with the following properties*: (i) *if we put, for a generic x over k on G,*

$F(x) = xa$, the mapping F of G onto H determines a one-to-one mapping of the cosets of $|Z|$ in G onto the points of H; (ii) *$k(x)$ is separable over $k(F(x))$*; (iii) *if ϕ is a mapping of G into a variety V, defined over an overfield K of k, and such that $\phi(xs) = \phi(x)$ whenever $s \in |Z|$ and x is generic over $K(s)$ on G, there is a mapping ψ of H into V, defined over K, such that $\phi = \psi \circ F$. If $|Z|$ is a normal subgroup of G, then one can define on H a group-law, defined over k, such that F is a homomorphism of G onto H.*

The "support" of a cycle was defined at the beginning of the Appendix of AG. The assumption on $|Z|$ implies that Z has one and only one component Z_0 containing e, that this is a subgroup of G, and that all the components of Z are cosets of Z_0 in G. We apply Prop. 1 to the cycle Z on $S = G$, G acting on itself by the left-translations, and to the field k; if x is generic over k on G, the smallest extension of k over which xZ is rational is contained in $k(x)$, and hence, by AG-App., Prop. 3, Coroll., it is regular over k. Therefore, by Prop. 1, there is a homogeneous space with respect to G, which we now call H, defined over k, and a mapping F of G into H, defined over k, with the properties stated in Prop. 1; in particular, F is everywhere defined, $t = F(x)$ is generic over k on H, and $k(t)$ is the smallest extension of k over which xZ is rational. If we put $a = F(e)$, a is rational over k, and we have, for all $s \in G$, $F(s) = sa$. If s, s' are any two points on G, we have $sa = s'a$ if and only if $sZ = s'Z$, i.e. if and only if $s^{-1}s'Z = Z$; by the assumption on Z, the latter relation is equivalent to $s^{-1}s' \in |Z|$. Thus the points of H are in a one-to-one correspondence with the cosets of $|Z|$ in G.

Call Γ the graph of F on $G \times H$. For any $b \in H$, $\Gamma \cap (G \times b)$ is the set of those points (s, b) which are such that $sa = b$; in particular, if x is generic over k on G and if we put $t = F(x) = xa$, $\Gamma \cap (G \times t)$ is the set of the points (s, t) such that $sa = xa$, i.e. $x^{-1}s \in |Z|$; this set can be written as $|xZ| \times t$. As $\Gamma \cdot (G \times t)$ is the prime rational cycle over $k(t)$ on $G \times H$ with the generic point (x, t) over $k(t)$, this shows that the prime rational cycle Z' over $k(t)$ on G with the generic point x has the same components as the cycle xZ; as the latter is rational over $k(t)$ and its components have the coefficient 1, this implies that $Z' = xZ$. As the components of the prime rational cycle with the generic point x over $k(t)$ have the coefficient 1, $k(x)$ must be separable (i.e. "separably generated") over $k(t)$.

As to (iii), let x be generic over K on G; put $t = F(x)$ and $w = \phi(x)$; let w' be any generic specialization of w over $K(t)$; this can be extended to a generic specialization x' of x over $K(t)$; we have then $w' = \phi(x')$

and $t = F(x')$, and the latter relation implies that x' is on $|xZ|$, i.e. that it is of the form xs with $s \in |Z|$. Let $\bar{x}$ be generic on G over $K(s)$; we have $\phi(\bar{x}s) = \phi(\bar{x})$; specializing $\bar{x}$ to x over $K(s)$, we get $\phi(xs) = \phi(x)$, since both sides are defined, i.e. $w' = w$. This shows that w is purely inseparable over $K(t)$; as it is at the same time rational over $K(x)$ which is separable over $K(t)$, it is therefore rational over $K(t)$, and we may write $w = \psi(t)$, where ψ is a mapping of H into V, defined over K. This proves (iii).

Finally, assume that $|Z|$ is a normal subgroup of G; let x, y be independent generic points of G over k; put $t = F(x)$, $u = F(y)$. We have $F(xy) = xF(y) = xu$; this is a function of x, defined over $k(u)$. If $s \in |Z|$, we have $xsy = xys'$ with $s' = y^{-1}sy \in |Z|$, and therefore $F(xsy) = F(xy)$; by (iii) applied to the mapping $x \to xu$ of G into H and to $K = k(u)$, this implies that $F(xy)$ is rational over $k(u,t)$. Therefore the mapping $u \to xu$ of H into H is defined over $k(t)$; on the other hand, if k' is any field of definition for that mapping, containing k, the image $xa = t$ of a by it is rational over k', so that $k(t) \subset k'$; thus $k(t)$ is the smallest field of definition for the mapping $u \to xu$. This shows that G is not operating faithfully on H; applying Prop. 2 of AG, no. 3, to G and H, we see that we can define on H a normal law of composition f such that $F(xy) = f(F(x), F(y))$. By the main theorem of AG, we can then replace H by a birationally equivalent group H', defined over k, with a mapping F' of G into H', also defined over k, such that $F'(xy) = F'(x)F'(y)$, $F(x)$ and $F'(x)$ being corresponding generic points of H and H' over k when x is generic over k on G. As usual, from the relation $F'(x) = F'(y)^{-1}F'(yx)$ which holds for x, y generic and independent over k, we deduce that F' is everywhere defined[1]; therefore, if G is made to operate on H' by the law $(x, w) \to F'(x)w$ for x, w generic and independent over k on G and H', H' is a homogeneous space with respect to G. But then the unicity assertion in the main theorem of AG can be applied to H and H' and shows that they are biregularly equivalent; in other words, H itself, with the law f, is a group. This completes the proof.

It is easily seen that the pair (H, a) is uniquely determined, up to an isomorphism, by the conditions (i), (ii), (iii) in Prop. 2; in other words, if H' and a' have similar properties, there is an everywhere biregular birational correspondence between H and H' which maps a onto a' and transforms the law of composition between G and H into the law between G and H'. The space H may be called the *coset-space* determined by G and Z, and may be denoted by G/Z; if $|Z|$ is a normal subgroup of G, the space H, with the group-law

[1] This is Theorem 1 of Nakano ([2]).

determined by Prop. 2, is called the *quotient-group* (or factor-group) of G by Z, and is denoted by G/Z.

3. Before making another application of Prop. 1, we will introduce a new condition which a law of composition may satisfy. Let V, W be two varieties, g a mapping of $V \times W$ into W, and k a field of definition for V, W and g; consider the following condition:

(TG 1′) *If x, u are independent generic points of V, W over k, and $v = g(x,u)$, then $k(x,u) = k(x,v) = k(u,v)$.*

The condition $k(x,u) = k(x,v)$ is equivalent to (TG 1) of AG, no. 2. The condition $k(x,u) = k(u,v)$ implies that the dimension of V, which is the dimension of x over $k(u)$, is the same as that of v over $k(u)$, and therefore at most that of W; if the dimensions of V and of W are the same, this implies that v is generic over $k(u)$ on W, which is condition (H) of AG, no. 2. Let k' be any field of definition containing k for the birational correspondence $u \to v = g(x,u)$ between W and itself; if u is taken generic over $k'(x)$ on W, we have $k'(u) = k'(v)$; since $k(x) \subset k'(u,v)$ by (TG 1′), we have $k(x) \subset k'(u)$. Taking u' generic on W over $k'(x,u)$, we get in the same manner $k(x) \subset k'(u')$. As $k'(u)$, $k'(u')$ are independent regular extensions of k', their intersection is k', so that $k(x) \subset k'$. This shows that (TG 1′) implies (TG 3). In view of the results of AG, end of no. 3, this shows that, if g satisfies (TG 1′) and (TG 2′), or if two mappings f, g of $V \times V$ into V and of $V \times W$ into W are given and satisfy (TG 1′, 2), then V is a pre-group and W a pre-transformation space, and V operates faithfully on W.

If a pre-group V and a pre-transformation space W satisfy (TG 1′), we say that W is a *pre-principal space* with respect to V; if at the same time V and W have the same dimension, so that, as we have shown, W is pre-homogeneous with respect to V, we also say that V is *simply pre-transitive on W*.

Let W be a pre-principal space with respect to a pre-group V; by the main theorem of AG, we can construct a group G and a transformation-space S, birationally equivalent to V, W and defined over the same field k; then S is also pre-principal with respect to G. Let T be the locus of (u, xu) over k on $S \times S$, x and u being independent generic points of G, S over k; put $t = (u, xu)$; then (TG 1′) implies that $k(x) \subset k(t)$, i.e. that we may write $x = \phi(t)$, where ϕ is a mapping of T into G, defined over k; conversely, if this is so for a transformation-space S with respect to G, S is pre-principal.

The space S will be called a *principal space with respect to* G if, for x, u generic and independent over k on G, S and for $t = (u, xu)$, we have $x = \phi(t)$ where ϕ is an *everywhere defined mapping*, defined over k, of the locus T of t over k into the group G. If at the same time S is homogeneous, it will be called a *principal homogeneous space* with respect to G.

PROPOSITION 3. *Let S be a pre-principal transformation-space with respect to a group G, both being defined over a field k. Then there is a k-open subset P of S which is a principal transformation-space with respect to G; if G and S have the same dimension, P is uniquely determined and is homogeneous.*

Let T and ϕ be defined as above; call F the k-closed subset of T where ϕ is not defined. We first show that, if (a, b) is in F, $(sa, s'b)$ is in F for all s, s' in G. In fact, take x, u generic and independent over $k(s, s')$ on G, S; put $v = xu$, $u_1 = su$, $v_1 = s'v$, $x_1 = s'xs^{-1}$; then we have $v_1 = x_1u_1$, and x_1, u_1 are generic and independent over $k(s, s')$ on G, S, so that (u, v) and (u_1, v_1) are generic points of T over $k(s, s')$, and that $x = \phi(u, v)$, $x_1 = \phi(u_1, v_1)$ by the definition of ϕ; this gives

$$\phi(u, v) = s'^{-1}\phi(su, s'v)s.$$

If (a, b) is in T, it is a specialization of (u, v) over $k(s, s')$, and therefore $(sa, s'b)$ is also in T; then the above relation shows that ϕ is defined at (a, b) if it is defined at $(sa, s'b)$, i. e. that $(a, b) \in F$ implies $(sa, s'b) \in F$.

As (e, u) is a specialization of (x, u) over k, e being the neutral element of G, T contains the diagonal Δ of $S \times S$. As the projection of Δ on either factor of $S \times S$ is everywhere biregular, the projection of the k-closed subset $F \cap \Delta$ of Δ onto S is a k-closed subset F' of S, consisting of the points $a \in S$ such that ϕ is not defined at (a, a). From what we have proved above, it follows that, if $a \in F'$, $sa \in F'$ for all $s \in G$. For the same reason, if a is in $S - F'$, then $\phi(a, sa)$ is defined for all $s \in G$; as (a, sa, s) is then a specialization of (u, xu, x) over k, and $x = \phi(u, xu)$, this shows that $\phi(a, sa) = s$ for all $a \in S - F'$ and all $s \in G$, and therefore $k(a, s) = k(a, sa)$; in particular, if x is generic over $k(a)$ on G, the locus of xa over $k(a)$ has a dimension equal to that of G.

If G is complete, every specialization (a, b) of (u, xu) over k can be extended to a specialization (a, b, s) of (u, xu, x) over k, so that $b = sa$; in other words, every point of T must be of the form (a, sa), with $a \in S$ and $s \in G$; then it follows from what we have proved above that such a point cannot be in F unless a and sa are in F'. Without attempting to decide whether this is still so in the general case, we shall merely show that, if u

is generic over k on S and (u, u') is in F, then u' must be in F'. In fact, suppose that this is not so; take x generic over $k(u, u')$ on G; call X, X' the loci of xu, xu' over $k(u, u')$ on S; by what we have proved above, they have the same dimension, which is that of G. By F-VI$_3$, Th. 11, we have $T \cap (u \times S) = u \times X$; at the same time, since we have shown that (u, xu') is in T, $u \times X'$ is contained in $T \cap (u \times S)$; as X and X' have the same dimension, this implies that $X = X'$. But, as we have shown, since (u, u') is in F, (u, xu') must be in F, and therefore, since F is k-closed, $u \times X'$ must be contained in F; as $X = X'$, this implies that F contains (u, xu), which is generic on T over k, and contradicts the definition of F. One may observe that, if S is pre-homogeneous, this again shows that (a, b) cannot be in F unless a, b are in F'; for, if $a \notin F'$ and x is generic on G over $k(a, b)$, xa has then over $k(a)$ a dimension equal to that of G, and therefore is generic on S over $k(a)$ since in the present case the dimensions of S and G are equal; then if (a, b) is in F, so is (xa, b), and so b must be in F'.

Now replace first S by $S - F'$; as F' is mapped onto itself by all operations of G, $S - F'$ is again a transformation-space with respect to G, defined over k, and satisfies our other assumptions. Writing again S instead of $S - F'$, we see that it is enough to prove our result under the additional assumption that $F' = \emptyset$. If G is complete or S is prehomogeneous, this already implies that S is principal. Otherwise we observe that, since T is also the locus of $(x^{-1}u, u)$ over k and since we have $\phi(x^{-1}u, u) = x$, T and F are mapped onto themselves by the mapping $(u, v) \to (v, u)$ of $S \times S$ onto itself. Call now F'' the "projection" of F on either factor of $S \times S$ (in the sense of F-IV$_3$ and F-VII$_3$, i. e. the closure of the set-theoretic projection); this will be the same, whether we project F onto the first or the second factor, and it is not S by what we have proved above, since F' is empty; it is therefore a k-closed subset of S. By what we have proved, F'' is mapped onto itself by all operations of G. Then $S - F''$ is the principal space whose existence was to be proved.

Finally, assume that the space S from which we first started was pre-homogeneous; this means that $T = S \times S$. Let a, b be any two points in $S - F'$; then, if x is generic on G over $k(a, b)$, xa, xb are generic on S over $k(a, b)$, and so there is an isomorphism σ of $k(a, b, xa)$ onto $k(a, b, xb)$ over $k(a, b)$, mapping xa onto xb; then we have $x^\sigma a = xb$, i. e. $b = x^{-1}x^\sigma a$. This shows that $S - F'$ is homogeneous, and also that an open subset of S which is a transformation-space for G cannot contain a point of $S - F'$ without containing $S - F'$. Therefore $S - F'$ is the only open subset of S which is a principal space with respect to G.

If S is a principal homogeneous space, the mapping ϕ of $T = S \times S$ into G which has been defined above will be called the *canonical mapping* of $S \times S$ into G. For any a, b on S and s on G, the relations $b = sa$, $s = \phi(a, b)$ are equivalent; in particular, for any a on S and for x generic over $k(a)$ on G, the mapping $x \to xa = v$ of G into S has the inverse $v \to x = \phi(a, v)$; as both are everywhere defined, this is therefore an everywhere biregular mapping of G onto S, defined over $k(a)$. In particular, if there is at least one rational point a over k on S, S is biregularly equivalent to G over k.

4. Let G be a group, V and W two varieties, and F a mapping of $V \times W$ into G, all defined over a field k. We may consider $W \times G$ as a transformation-space with respect to G, the law of composition between them being $(x, (N, y)) \to (N, xy)$ for any N in W and any x, y in G. We now apply Prop. 1 of no. 1 to the case when we take for S this transformation-space $W \times G$ and for Z the graph of the mapping $N \to F(M, N)$ of W into G, where M, N are independent generic points of V, W over k. We must then consider the smallest field of definition k' containing k for the mapping $N \to xF(M, N)$ of W into G, where x is generic over $k(M, N)$ on G. As this mapping is defined over $k(x, M)$, k' is a regular extension of k, contained in $k(x, M)$. Then Prop. 1 shows that we may write $k' = k(u)$, where u is a generic point over k of a transformation-space U with respect to G; as $k(u) \subset k(x, M)$, we may write $u = f(x, M)$, where f is a mapping of $G \times V$ into U, defined over k; moreover, as the mapping $x \to f(x, M)$ of G into U is no other than the mapping F defined in Prop. 1, we see that f is defined at every point (s, M) of $G \times M$, and that $f(ss', M) = sf(s', M)$; taking $s' = e$, and writing $f(M)$ instead of $f(e, M)$, this gives $f(s, M) = sf(M)$, and in particular $u = xf(M)$. As the mapping $N \to xF(M, N)$ is defined over $k(u)$, $xF(M, N)$ is rational over $k(u, N)$; similarly, if y is generic over $k(x, M, N)$ on G, the mapping $N \to yxF(M, N)$ is defined over $k(yu)$, and so $yxF(M, N)$ is rational over $k(yu, N)$. As we can write

$$y = (yxF(M, N))(xF(M, N))^{-1},$$

this shows that y is rational over $k(u, yu, N)$. If N' is generic on W over $k(x, y, M, N)$, y must then also be rational over $k(u, yu, N')$; thus $k(y)$ is contained in $k(u, yu, N)$ and in $k(u, yu, N')$; as these are independent regular extensions of $k(u, yu)$, their intersection is $k(u, yu)$, and so we have $k(y) \subset k(u, yu)$. This means that U is a pre-principal space and may therefore, by Prop. 3, be replaced by a principal space, birationally equivalent to it.

The most interesting case is that in which there are two mappings F_1, F_2 of V, W into G, defined over some overfield K of k, such that $F(M,N) = F_1(M)F_2(N)$ for M, N generic and independent over K on V, W; by the corollary of Th. 7, VA-18, this is always so whenever G is an abelian variety. Take x generic over $K(M,N)$ on G, and put $z = xF_1(M)$; then the mapping $N \to xF(M,N) = zF_2(N)$ is defined over $K(z)$, so that $k(u) \subset K(z)$. As x, M are generic and independent over $K(N)$ on G, V, u is then generic over $K(N)$ on U, and the dimension of U is that of u over K; the relation $K(u) \subset K(z)$ shows that this is at most the dimension of G. Therefore U is pre-homogeneous and may be taken to be a principal homogeneous space with respect to G. Moreover, we may write $u = \Phi(z)$, where Φ is a mapping of G into U, defined over K. If we substitute yx for x, with y generic over $K(M,N,x)$ on G, z is replaced by yz, and u by yu; this gives $\Phi(yz) = y\Phi(z)$, which may be written as $\Phi(z) = y^{-1}\Phi(yz)$ and thus shows that Φ is everywhere defined. Putting now $a = \Phi(e)$, we see that a is rational over K and that $u = za$, i. e. $f(M) = F_1(M)a$. Put now $g(N) = F_2(N)^{-1}a$; g is a mapping of W into U, defined over K. As we have also $g(N) = F(M,N)^{-1}f(M)$, g is also defined over the field $k(M)$, and therefore also over $k(M')$ if M' is another generic point of V over K; if we take M, M' generic and independent over K on V, $k(M)$ and $k(M')$ are independent regular extensions of k, so that their intersection is k; hence g is defined over k. Thus we have proved the following result:

PROPOSITION 4. *Let G be a group, V and W two varieties and F a mapping of $V \times W$ into G, all defined over k. Assume that there are two mappings F_1, F_2 of V, W into G, defined over some overfield K of k, such that $F(M,N) = F_1(M)F_2(N)$ for M, N generic and independent over K on V, W. Then there is a principal homogeneous space U with respect to G, and two mappings f, g of V, W into U, all defined over k, such that $f(M) = F(M,N)g(N)$, i. e. $F(M,N) = \phi(g(N),f(M))$, where ϕ is the canonical mapping of $U \times U$ into G.*

COROLLARY. *Notations being as in Prop. 4, U, f and g are uniquely determined by G, V, W and F, up to an isomorphism.*

In fact, assume that U', f', g' have similar properties; then we have $xF(M,N) = \phi'(g'(N), xf'(M))$, where ϕ' is the canonical mapping for U'. This shows that the mapping $N \to xF(M,N)$ is defined over $k(u')$ with $u' = xf'(M)$; thus, if we put $u = xf(M)$ as before, we have $k(u) \subset k(u')$ and may write $u = \psi(u')$, where ψ is a mapping of U' into U, defined over k.

Replacing x by yx, with y generic on G over $k(M, N, x)$, we get $yu = \psi(yu')$; from this we conclude, in the usual manner, that ψ is everywhere defined. Take any point a' on U', and put $a = \psi(a')$; as we have $xa = \psi(xa')$, and as the mappings $x \to xa$, $x \to xa'$ are everywhere biregular mappings of G onto U and U', defined over $k(a')$, we see that ψ is an everywhere biregular mapping of U' onto U. Moreover, we have $\psi(u') = x\psi(f'(M))$, and therefore $f = \psi \circ f'$; from this one easily concludes that $g = \psi \circ g'$. This proves our assertion.

5. Let G be a group, defined over a field k. We will now prove that the classes of principal homogeneous spaces with respect to G, for birational equivalence over k, form a set. In fact, let x, y be independent generic points of G over k; let σ be the isomorphism of $\bar{k}(x)$ onto $\bar{k}(yx)$ over $\bar{k}$ which maps x onto yx. Let H be any principal homogeneous space with respect to G, defined over k; let a be an algebraic point over k on H, and put $u = xa$, so that u is generic over k on H. Then $k(u)$ is a regular extension of k contained in $\bar{k}(x)$ and such that $\bar{k}(u) = \bar{k}(x)$; moreover, we have

$$k(y, u) = k(y, u^\sigma) = k(u, u^\sigma)$$

since $u^\sigma = yu$. Conversely, let $k(u)$ be any such extension of k, and call U the locus of u over k; then we may write $u^\sigma = g(y, u)$, where g is a mapping of $G \times U$ into U, defined over k; and one verifies at once that this makes U into a pre-principal pre-homogeneous space with respect to G, and thus determines uniquely a class of birationally equivalent principal homogeneous spaces with respect to G. As every such class is determined by at least one such extension, this shows that these classes form a set.

If G is commutative, one can define canonically a commutative group-structure on the set of classes of principal homogeneous spaces with respect to G. In order to do this, we first observe that, if H is any transformation-space over a commutative group G, then the law $(x, u) \to x^{-1}u$, for $x \in G$, $u \in H$, defines on H a structure of transformation-space with respect to G; this will be called the *opposite* transformation-space to H and will be denoted by H^-; it is a principal homogeneous space if H is such.

PROPOSITION 5. *Let G be a commutative group, defined over a field k. Let H_i, for $1 \leqq i \leqq n$, be principal homogeneous spaces with respect to G, defined over k. Then there is a principal homogeneous space H with respect to G, defined over k, and an everywhere defined mapping f of $H_1 \times H_2 \times \cdots \times H_n$ into H, defined over k, such that*

$$f(s_1a_1, \cdots, s_na_n) = s_1 \cdots s_nf(a_1, \cdots, a_n)$$

for all $s_i \in G$ *and* $a_i \in H_i$. *Moreover,* H *and* f *are uniquely determined up to an isomorphism of* H.

Put $V = W = H_1 \times H_2 \times \cdots \times H_n$; call ϕ_i the canonical mapping of $H_i \times H_i$ into G, so that $b_i = sa_i$ is equivalent to $s = \phi_i(a_i, b_i)$ for a_i, b_i in H_i and s in G. Let $u = (u_1, \cdots, u_n)$ and $v = (v_1, \cdots, v_n)$ be two points of V; put

$$F(u, v) = \prod_{i=1}^{n} \phi_i(u_i, v_i),$$

where the right-hand side has a meaning since G is commutative. On each H_i, choose a point a_i, and put $a = (a_1, \cdots, a_n)$. We have

$$\phi_i(u_i, v_i) = \phi_i(a_i, v_i)\phi_i(a_i, u_i)^{-1}$$

for all i, as one verifies at once, and therefore, again because of the commutativity of G:

$$F(u, v) = F(a, v)F(a, u)^{-1}.$$

Thus the assumptions of Prop. 4 are satisfied, so that there is a principal homogeneous space U and two mappings f, g of V into U, all defined over k, such that

$$(1) \qquad f(u) = F(u, v)g(v), \qquad F(u, v) = \phi(g(v), f(u)),$$

where ϕ is the canonical mapping of $U \times U$ into G. Take any point b on V, and take v generic over $k(b)$ on V; as F is defined at (b, v), the relation (1) shows that f is defined at b. Thus f is everywhere defined. As $F(u, u) = e$, the relation (1) gives $g(u) = f(u)$, i.e. $f = g$. If $s_1, \cdots, s_n$ are any elements of G, and we put $s = s_1 \cdots s_n$ and $u' = (s_1u_1, \cdots, s_nu_n)$, we have $F(u', v) = s^{-1}F(u, v)$ and therefore, by (1), $f(u') = s^{-1}f(u)$. If we now put $H = U^-$, i.e. if we take for H the opposite space to U, H and f will have the properties stated in Prop. 5.

Let us now assume that $\bar{H}$ and $\bar{f}$ have similar properties; put $\bar{U} = \bar{H}^-$. Put $\bar{z} = F(u, v)^{-1}\bar{f}(u)$, the multiplication in the right-hand side being that of $\bar{U}$. If the s_i, s and u' have the same meaning as above, we have $\bar{f}(u') = s^{-1}\bar{f}(u)$, so that $\bar{z}$ does not change if one replaces u, v by u', v. Therefore $k(\bar{z})$ is contained both in $k(u, v)$ and in $k(u', v)$. If the s_i have been taken generic and independent over $k(u, v)$ on G, $k(u, v)$ and $k(u', v)$ will be independent regular extensions of $k(v)$; this gives $k(\bar{z}) \subset k(v)$, so that we may write $\bar{z} = \bar{g}(v)$, with $\bar{g}$ defined over k. Then we have $\bar{f}(u) = F(u, v)\bar{g}(v)$; by the corollary of Prop. 4, $\bar{U}$, $\bar{f}$ and $\bar{g}$ must then be

the same as U, f and f, respectively, except for an isomorphism of U onto $\bar{U}$. This proves the assertion about unicity in Prop. 5.

In Prop. 5, take $n=2$; call $\mathfrak{H}_1$, $\mathfrak{H}_2$ the classes of H_1, H_2, and denote by $\mathfrak{H}_1+\mathfrak{H}_2$ the class of H. This defines on the set of classes of principal homogeneous spaces with respect to G a commutative group-structure. In fact, commutativity is obvious. Call $\mathfrak{H}_0$ the class of G, and therefore of all principal homogeneous spaces with respect to G which have a rational point over k. For any principal homogeneous space H with respect to G, the mapping $f(x,u)=xu$ of $G\times H$ into H satisfies the condition of Prop. 5; therefore we have $\mathfrak{H}_0+\mathfrak{H}=\mathfrak{H}$ for all classes $\mathfrak{H}$. If ϕ is the canonical mapping of $H\times H$ into G, then ϕ, considered as a mapping of $H\times H^-$ into G, satisfies the condition of Prop. 5; therefore, if $\mathfrak{H}^-$ is the class of H^-, we have $\mathfrak{H}+\mathfrak{H}^-=\mathfrak{H}_0$. Finally, let H_1, H_2, H_3 be three principal homogeneous spaces with respect to G; apply Prop. 5 successively to the following spaces: (a) to H_1, H_2, obtaining a space H_{12} and a mapping f_{12}; (b) to H_{12}, H_3, obtaining H', f'; (c) to H_2, H_3, obtaining H_{23}, f_{23}; (d) to H_1, H_{23}, obtaining H'', f''; (e) to H_1, H_2, H_3, obtaining H, f. Then the two mappings

$$f'(f_{12}(u_1,u_2),u_3),\qquad f''(u_1,f_{23}(u_2,u_3))$$

of $H_1\times H_2\times H_3$ into H', H'' satisfy the same condition as the mapping f. By the unicity assertion of Prop. 5, this shows that H', H'' are isomorphic to H. This means that the addition $\mathfrak{H}_1+\mathfrak{H}_2$ is associative.

One proves quite similarly, by induction on n, that if $\mathfrak{H}$ and $\mathfrak{H}_i$ are the classes of the spaces H, H_i in Prop. 5, then $\mathfrak{H}=\sum_i \mathfrak{H}_i$. In fact, let H', f' be the space and the mapping obtained by applying Prop. 5 to $H_1,\cdots,H_{n-1}$, so that $\mathfrak{H}'=\mathfrak{H}_1+\cdots+\mathfrak{H}_{n-1}$ by the induction assumption; and let H'', f'' be the space and the mapping obtained by applying Prop. 5 to H', H_n, so that $\mathfrak{H}''=\mathfrak{H}'+\mathfrak{H}_n$ by definition. Then the mapping

$$(u_1,\cdots,u_n)\to f''(f'(u_1,\cdots,u_{n-1}),u_n)$$

of $H_1\times\cdots\times H_n$ into H'' has the properties stated for f in Prop. 5, so that, by the unicity assertion in Prop. 5, H'' is isomorphic to H.

From this one deduces that every element $\mathfrak{H}$ of the group we have just described is of finite order. In fact, take on a space H of class $\mathfrak{H}$ any positive cycle $\sum_{i=1}^{n} a_i$ of dimension 0, rational over k. Call H_n any space of class $n\mathfrak{H}$; then there is a mapping $f(u_1,\cdots,u_n)$ of the product of n factors equal to H into H_n with the properties stated in Prop. 5. From the unicity assertion in Prop. 5, it follows that any permutation of the u_i will change f

into sf, with $s \in G$; as f is everywhere defined, we see that $s = e$ by taking $u_1 = \cdots = u_n$; therefore f is a symmetric function, so that $f(a_1, \cdots, a_n)$ is rational by the main theorem on symmetric functions (VA-7, Th. 1). So H_n has a rational point over k, and is therefore isomorphic to G.

Now, $\mathfrak{A}$ being as before, put $H_0 = G$ and take, for each integer $n \neq 0$, a space H_n of class $n\mathfrak{A}$ so that all the H_n are disjoint. On the set $\mathfrak{G} = \bigcup_n H_n$ (which is of course not an algebraic variety), we will define a commutative group-law f (in the sense of group-theory, not of algebraic geometry) such that $H_0 = G$ will be a subgroup of $\mathfrak{G}$ and that f induces on $H_m \times H_n$, for all m, n, a mapping $f_{m,n}$ of $H_m \times H_n$ into H_{m+n} satisfying the conditions in Prop. 5. As there is such a mapping $f_{m,n}$ for each m, n, and as it is uniquely determined up to an automorphism of H_{m+n} (i.e. up to left-multiplication by a rational point of G), we merely have to choose the $f_{m,n}$ so that the mapping f of $\mathfrak{G} \times \mathfrak{G}$ into $\mathfrak{G}$ which coincides with $f_{m,n}$ on $H_m \times H_n$ for all m, n satisfies the axioms for groups; we do this as follows. For any n, we take $f_{0,n}(x, u) = xu$ for $x \in G$, $u \in H_n$. We choose $f_{-1,1}$ and, for all $n > 0$, $f_{n,1}$ and $f_{-n,-1}$ so as to satisfy the conditions in Prop. 5. Now, for elements $u_1, \cdots, u_{n+1}$ of H_1 in any number, we define $u_1 \cdots u_{n+1}$ inductively as being equal to u_1 for $n = 0$ and to $f_{n,1}(u_1 \cdots u_n, u_{n+1})$ for $n \geqq 1$; similarly, for elements $v_1, \cdots, v_{n+1}$ of H_{-1}, we define $v_1 \cdots v_{n+1}$ as equal to v_1 for $n = 0$ and to $f_{-n,-1}(v_1 \cdots v_n, v_{n+1})$ for $n \geqq 1$. It is then easily seen that, whenever m, n are both > 0, there is one and only one way of choosing $f_{m,n}$ so that it satisfies the condition

$$f_{m,n}(u_1 \cdots u_m, u_{m+1} \cdots u_{m+n}) = u_1 \cdots u_{m+n}$$

when the u_i are in H_1; we determine $f_{-m,-n}$ similarly, using H_{-1} instead of H_1. Finally, for $m \geqq n > 0$, we choose $f_{m,-n}$ and $f_{-m,n}$ so as to satisfy the conditions

$$f_{m,-n}(u_1 \cdots u_m, v_1 \cdots v_n) = \prod_{i=1}^{n} f_{-1,1}(v_i, u_i) \cdot u_{n+1} \cdots u_m$$

$$f_{-m,n}(v_1 \cdots v_m, u_1 \cdots u_n) = \prod_{i=1}^{n} f_{-1,1}(v_i, u_i) \cdot v_{n+1} \cdots v_m$$

respectively, the u_i being any elements of H_1 and the v_i any elements of H_{-1}. It is then a trivial matter to verify that these choices of the $f_{m,n}$ satisfy all the requirements for a commutative group-law on $\mathfrak{G}$.

The points on the H_n which are rational over k form a subgroup $\mathfrak{g}$ of $\mathfrak{G}$. As we have shown that there are such points for some $n \neq 0$, there is a smallest $n > 0$ for which there is such a point $a \in H_n$; this n is the order of $\mathfrak{A}$ in the group of classes of principal homogeneous spaces with respect to G. Then $\mathfrak{g}$ is the direct product of the group $\mathfrak{g}_0 = \mathfrak{g} \cap G$ of rational

points over k on G and of the infinite cyclic group γ generated by a. The quotient-group $\mathfrak{G}/\gamma$ may be described as an algebraic group consisting of n components respectively isomorphic to $H_0 = G, H_1, \cdots, H_{n-1}$.

6. PROPOSITION 6. *Let A be an abelian variety and H a principal homogeneous space with respect to A, both being defined over a field k. Let $V_1, \cdots, V_n$ be varieties, and F a mapping of $V_1 \times \cdots \times V_n$ into H, all these being defined over k. Then there is for each i a principal homogeneous space H_i with respect to A and a mapping F_i of V_i into H_i, H_i and F_i being defined over k, and there is a mapping f of $H_1 \times \cdots \times H_n$ into H with the properties stated in Prop. 5, such that, for $(M_1, \cdots, M_n)$ generic over k on $V_1 \times \cdots \times V_n$, we have*

$$F(M_1, \cdots, M_n) = f(F_1(M_1), \cdots, F_n(M_n)).$$

Moreover, all these are uniquely determined up to isomorphisms.

For $n = 1$, there is nothing to prove. If the assertion is proved for a product of two factors, then this can be applied to the product $V_1 \times (V_2 \times \cdots \times V_n)$ of V_1 and $V_2 \times \cdots \times V_n$, so that the general case follows by induction on n. Thus it is enough to treat the case of two factors V, W and of a mapping F of $V \times W$ into H. Call ϕ the canonical mapping of $H \times H$ into A; let (M, N) and (M', N') be two independent generic points of $V \times W$ over k; and put

$$x = \phi(F(M, N'), F(M', N')), \qquad y = \phi(F(M, N), F(M, N')).$$

so that we have

$$xy = \phi(F(M, N), F(M', N')).$$

As the mapping $((M, M'), N') \to x$ of $(V \times V) \times W$ into A has the constant value e on the variety $(M, M) \times W$, Th. 7 of VA-18 shows that x is rational over $k(M, M')$; for a similar reason, y must be rational over $k(N, N')$; in other words, there are mappings Φ, Ψ of $V \times V$, $W \times W$ into A, both defined over k, such that $x = \Phi(M, M')$ and $y = \Psi(N, N')$. By the corollary of Th. 7 of VA-18, Φ and Ψ satisfy the assumptions of Prop. 4, so that there are two principal homogeneous spaces U_1, U_2 with respect to A, mappings F_1, G_1 of V into U_1 and mappings F_2, G_2 of W into U_2, all defined over k, such that $F_1(M) = xG_1(M')$, $F_2(N) = yG_2(N')$; moreover, as $\Phi(M, M)$, $\Psi(N, N)$ are defined and equal to e, we have $G_1 = F_1$, $G_2 = F_2$. Now call H_1, H_2 the spaces respectively opposite to U_1, U_2, and apply Prop. 5 to H_1, H_2: let $\bar{H}$ be the principal homogeneous space and $\bar{f}$ the mapping of $H_1 \times H_2$ into $\bar{H}$ with

the properties stated in that proposition. Put $\bar{F}(M,N) = \bar{f}(F_1(M), F_2(N))$. As H_1, H_2 are opposite to U_1, U_2, we have

$$F_1(M') = xF_1(M), \qquad F_2(N') = yF_2(N),$$

multiplication in the right-hand sides being understood in the sense of H_1, H_2. By the definition of $\bar{f}$, we have then:

$$\bar{F}(M',N') = (xy)\bar{F}(M,N),$$

while, as we have seen above, the same relation holds if F is substituted for $\bar{F}$. But then, as the corollary of Th. 7, VA-18, shows that the mapping

$$((M',N'),(M,N)) \to xy$$

of $(V \times W) \times (V \times W)$ into A satifies the condition of Prop. 4, the corollary of Prop. 4 shows that $\bar{H}$, $\bar{F}$ must be the same as H, F except for an isomorphism of H onto $\bar{H}$. Then, replacing $\bar{f}$ by a mapping f of $H_1 \times H_2$ into H by means of that isomorphism, we have the spaces H_1, H_2 and the mappings F_1, F_2, f whose existence was asserted in our proposition.

As to unicity, assume that there are spaces H_1^*, H_2^* and mappings F_1^*, F_2^*, f^* with the same properties. Then, x being defined as above, or equivalently by $F(M',N') = xF(M,N')$, we have

$$f^*(F_1^*(M'),F_2^*(N')) = xf^*(F_1^*(M),F_2^*(N')) = f^*(xF_1^*(M),F_2^*(N'))$$

and therefore $F_1^*(M') = xF_1^*(M)$ since the mapping $u \to f^*(u,v)$ of H_1^* into H is, as easily seen, an everywhere biregular mapping of H_1^* onto H. But then the corollary of Prop. 4, applied to the mapping $(M',M) \to x$ of $V \times V$ into A, shows that H_1^*, F_1^* are the same as H_1, F_1 except for an isomorphism. The same argument applied to y instead of x shows that H_2, F_2 are uniquely determined up to an isomorphism. Then Prop. 5 shows that f is uniquely determined. This completes the proof.

7. The foregoing results will now be applied to the theory of Jacobian varieties. As in VA-35, we consider a complete non-singular curve Γ of genus $g > 0$, defined over a field k. If $\mathfrak{a}$ is any divisor on Γ, Prop. 6 of the Appendix of AG shows that there is a smallest field containing k over which $\mathfrak{a}$ is rational; this field will be denoted by $k(\mathfrak{a})$. In particular, if $M_1, \cdots, M_g$ are independent generic points of Γ over k and if we put $\mathfrak{m} = \sum_i M_i$, then, by VA-4, Lemma 1, $k(\mathfrak{m})$ is the field $k(M_1, \cdots, M_g)_s$ of symmetric functions of $M_1, \cdots, M_g$ defined over k, i.e. the subfield of $k(M_1, \cdots, M_g)$ consisting of those elements which are invariant under all permutations of

$M_1, \cdots, M_g$; such a divisor $\mathfrak{m}$ will be called generic over k. As $k(\mathfrak{m})$ is a regular extension of k, we may write it as $k(u)$, where u is a generic point of a variety W over k, and we may write $u = F(M_1, \cdots, M_g)$, with F defined over k; as F is symmetric in the M_i, this may also be written as $u = F(\mathfrak{m})$.

Now let the N_i, P_i, for $1 \leqq i \leqq g$, be $2g$ independent generic points of Γ over $k(\mathfrak{m})$; and put:

$$x = (N_1, \cdots, N_g, P_1, \cdots, P_g),$$

this being a generic point over k of the product $V = \Gamma \times \cdots \times \Gamma$ of $2g$ factors equal to Γ. By VA-35, Lemma 11, there is a positive divisor $\mathfrak{m}'$ on Γ linearly equivalent to $\mathfrak{m} + \sum_{i=1}^{g} N_i - \sum_{i=1}^{g} P_i$, and it is uniquely determined and such that $k(x, \mathfrak{m}) = k(x, \mathfrak{m}')$; this implies that it is generic over $k(x)$. Then, if we write $u' = F(\mathfrak{m}')$, we have $k(x, u) = k(x, u')$; we may thus write $u' = g(x, u)$, where g is a mapping of $V \times W$ into W which satisfies (TG 1).

We now show that this mapping satisfies the condition (TG 2′) of AG, no. 3, Prop. 2, so that this proposition may be applied to it. In fact, let y be a generic point of V over $k(x, u)$; we may write

$$y = (Q_1, \cdots, Q_g, R_1, \cdots, R_g).$$

Then the point $u'' = g(y, u')$ will be determined by $u'' = F(\mathfrak{m}'')$, where $\mathfrak{m}''$ is the positive divisor linearly equivalent to $\mathfrak{m}' + \sum_i Q_i - \sum_i R_i$. Applying again VA-35, Lemma 11, we see that there is a positive divisor $\sum_i S_i$ linearly equivalent to $\sum_i N_i - \sum_i P_i + \sum_i Q_i$, and that it is generic over $k(y, u)$ and rational over $k(x, y)$. But then $\mathfrak{m}''$ is linearly equivalent to $\mathfrak{m} + \sum_i S_i - \sum_i R_i$, which shows that, if we put

$$z = (S_1, \cdots, S_g, R_1, \cdots, R_g)$$

z is generic on V over $k(u)$ and that we have $u'' = g(z, u)$. This shows that g satisfies (TG 2′). Applying Prop. 2 of AG, no. 3 and the main theorem of AG, we see that there is a group J, a normal law $\bar{g}$ between J and W, and a mapping ϕ of V into J such that $g(x, u) = \bar{g}(\phi(x), u)$ for x, u generic and independent over k on V, W.

Put now $K = k(P_1, \cdots, P_g)$, $\mathfrak{n} = \sum_i N_i$, and

$$w = (S_1, \cdots, S_g, Q_1, \cdots, Q_g).$$

Since the P_i, Q_i, N_i are generic and independent over k, Lemma 11 of VA-35

shows that w is generic over K on V. At the same time, the linear equivalence by which the S_i were defined shows at once that $g(x,u) = g(w,u)$ for u generic over $k(x,w)$, and therefore $\bar{g}(\phi(x),u) = \bar{g}(\phi(w),u)$. Since J, by definition, operates faithfully on W, this implies $\phi(x) = \phi(w)$; as w is generic over K on V, this shows that $\phi(x)$ is generic over K on J. It will now be shown that $K(\phi(x)) = K(\mathfrak{n})$. In fact, if u and $u' = g(x,u)$ are as before, u' is rational over $K(\mathfrak{m},\mathfrak{n}) = K(u,\mathfrak{n})$ since the divisor $\mathfrak{m}'$ is so by Lemma 11 of VA-35; therefore the mapping $u \to u'$ is defined over $K(\mathfrak{n})$, so that $K(\phi(x)) \subset K(\mathfrak{n})$. Put now $K' = K(\phi(x))$, so that u' is rational over $K'(u)$; then $\mathfrak{m}$ and $\mathfrak{m}'$ are both rational over $K'(u)$. But Lemma 11 of VA-35 shows that $\mathfrak{n}$ is rational over $K(\mathfrak{m},\mathfrak{m}')$ and therefore over $K'(u)$. If u_1 is a generic point of W over $K'(u)$, $\mathfrak{n}$ will also be rational over $K'(u_1)$; as $K'(u)$, $K'(u_1)$ are independent regular extensions of K', this implies that $\mathfrak{n}$ is rational over K'.

But now a comparison with the construction of the jacobian variety given in VA-36 shows that the latter coincides with our J over a suitably extended groundfield; more precisely, substituting K for k, $\sum_i P_i$ for $\mathfrak{a}$, $\mathfrak{n}$ for $\mathfrak{m}$ and $\phi(x)$ for z in the treatment given in VA-36, we get the same law of composition for the field $K(\phi(x))$ as has been defined above. Alternatively, one may also reason as follows. Let J_1 be the jacobian variety as defined in VA; let ϕ_1 be the "canonical mapping" of Γ into J_1, also according to the definition of VA-37 (which will soon be replaced by a more appropriate one); let K_1 be an overfield of the field K defined above, over which J_1 and ϕ_1 are defined; take $\mathfrak{n}$ generic over K_1; put $t = \phi(x)$, x being as above, and $z = S[\phi_1(\mathfrak{n})]$. As we have then $K_1(x) = K_1(z) = K_1(\mathfrak{n})$, the mapping $x \to z$ defines a birational correspondence between J and J_1, defined over K_1. If we write it as $z = f(x)$, f is everywhere defined by VA-15, Th. 6; and this, by the results at the beginning of VA-19, must then be of the form $f(x) = f_0(x) + a$, where $a = f(e)$ and where f_0 is a homomorphism, so that (using the additive notation on J_1 and the multiplicative notation on J) we have $f_0(xx') = f_0(x) + f_0(x')$. But then f_0 is again a birational correspondence, and, if g is the inverse mapping to f_0, we have $g(z+z') = g(z)g(z')$ for z, z' generic and independent over K_1 on J_1. This can be written as $g(z) = g(z+z')g(z')^{-1}$; if then z_1 is any point of J_1, and we take z' generic on J_1 over $K_1(z_1)$, this shows that g is defined at z_1. As f_0, g are everywhere defined, they determine an isomorphism between J and J_1.

One could also, without making use of the results of VA, verify directly (for instance by making use of the criterion for the completeness of a group

given by VA-33, Th. 16) that the group J we have constructed here is complete and is therefore an abelian variety. Then the results we have proved above, combined with the corollary of Th. 7, VA-18, show at once that J has the properties stated in VA-36, Th. 18; since the whole theory of the jacobian variety depends upon nothing else, and these properties (as proved in VA-37) are characteristic of the jacobian variety, this would suffice for a complete treatment.

From this discussion, we conclude that J is an abelian variety. Now apply Prop. 6 to the mapping ϕ of V into J; this defines $2g$ mappings of Γ into principal homogeneous spaces with respect to J, all defined over k. As ϕ is symmetric in the N_i and also in the P_i, the unicity assertion in Prop. 6 shows at once that the first g mappings must coincide, and that the last g mappings must coincide; call F, F' these mappings, and H, H' the spaces into which they map Γ. Now, notations being the same as above in no. 6, put

$$x' = (P_1, \cdots, P_g, N_1, \cdots, N_g).$$

Then we have, always with the same notations as before, $u = g(x', u')$, and therefore $\phi(x') = \phi(x)^{-1}$. This, combined with the unicity assertion in Prop. 6, shows at once that H' is the opposite space to H while F' must be the same as F.

We now embed J and H, in the manner explained at the end of no. 5, into a commutative group $\mathfrak{G}$ consisting of principal homogeneous spaces H_n with respect to J, all defined over k, with $H_0 = J$, $H_1 = H$, in such a way that $\mathfrak{G}/J$ is an infinite cyclic group, that the H_n are the cosets of J in $\mathfrak{G}$ and that the group-law in $\mathfrak{G}$ induces on $H_m \times H_n$, for all m, n, a mapping of $H_m \times H_n$ into H_{m+n} defined over k and satisfying the conditions in Prop. 5. At the same time, we change from the multiplicative to the additive notation, not only in J but also in $\mathfrak{G}$. With this notation, we have, if x, $\phi(x)$ and F have the same meaning as before,

$$\phi(x) = \sum_i F(N_i) - \sum_i F(P_i).$$

Let us now extend the mapping F into a homomorphism of the group of divisors on Γ into $\mathfrak{G}$, by putting $F(\mathfrak{a}) = \sum_i n_i F(A_i)$ for any divisor $\mathfrak{a} = \sum_i n_i A_i$, so that $F(\mathfrak{a}) \in H_n$ if n is the degree of $\mathfrak{a}$; in particular, $F(\mathfrak{a})$ is in J if and only if $\mathfrak{a}$ is of degree 0. If a is any point of H and M is a generic point of Γ over $k(a)$, the mapping $M \to F(M) - a$ of Γ into J, which is defined over $k(a)$, is a "canonical mapping" in the sense of VA-37; naturally it is only defined up to an additive constant; and, by the unicity assertion in Prop. 6,

no such mapping can be defined over k unless H is isomorphic to G, i. e. unless H has a rational point over k. From Th. 19 of VA-38, one deduces immediately that a divisor $\mathfrak{a}$ on Γ is linearly equivalent to 0 if and only if $F(\mathfrak{a}) = 0$.

In other words, *the homomorphism* $\mathfrak{a} \to F(\mathfrak{a})$ *determines an isomorphism of the group of all divisor-classes* (of any degree) *on* Γ *onto the group* $\mathfrak{G}$. From the foregoing results, one concludes easily that these properties are characteristic for $\mathfrak{G}$ and F, up to isomorphisms on J and its cosets H_n in $\mathfrak{G}$. One may call $\mathfrak{G}$ the *Jacobian group of* Γ, and F the *canonical mapping* of Γ, and of the group of divisors on Γ, into the Jacobian group. In substance, the construction of the varieties H_n has already been given by Chow (in [1]) by a method belonging to projective geometry.

THE UNIVERSITY OF CHICAGO.

BIBLIOGRAPHY.

[1] W. L. Chow, "The Jacobian variety of an algebraic curve," *American Journal of Mathematics*, vol. 76 (1954), pp. 453-476.

[2] S. Nakano, "Note on group varieties," *Memoirs of the College of Science, University of Kyoto*, Series A, vol. 27 (1952), Math. no. 1, pp. 55-66.

[3] A. Weil, *Variétés abéliennes et courbes algébriques*, Paris, Hermann et Cie, 1948.

[4] ———, "On algebraic groups of transformations," *American Journal of Mathematics*, vol. 77 (1955), pp. 355-391.