Realization of Finite Groups over Function Fields

MOSHE JARDEN

The Hebrew University of Jerusalem

Communicated by A. Fröhlich

Received September 20, 1971

Douady proved in [3, p. 5306, Theorem 2] that if C is an algebraically closed field of characteristic zero, and t is a transcendental element over C, and Ω is the algebraic closure of $C(t)$, then the Galois group, $\mathcal{G}(\Omega/C(t))$ of Ω over $C(t)$, is isomorphic to the free profinite group generated by a set having the same cardinality as C. One can deduce immediately that every finite group is realizable over $C(t)$, i.e., for every finite group G there exists a Galois extension L of $C(t)$ such that $\mathcal{G}(L/C(t))$ is isomorphic to G. We shall refer to this conclusion in the sequel as Douady's theorem.

In this note we intend to transfer Douady's theorem to fields of prime characteristic. Indeed, we prove that for every finite group G there exists a finite set of primes A such that if p is a prime not in A, k is an algebraically closed field of prime characteristic, and t is a transcendental element over k, then G is realizable over $k(t)$. Also, there exists a set S of primes, of positive Dirichlet density, such that if $p \in S$ and k is either a field of characteristic p or a field which contains the field of p-adic numbers, Q_p, then G is realizable over $k(t)$.

Originally, I proved the results by using a "Translating Theorem" of mine (see [4]), but according to Professor Grothendieck's suggestion transmitted to me by Professor Kuyk, I have introduced a direct proof based on reduction theory.

The following conventions will be used in the sequel. If k is a field then k_s and $\tilde{k}$ will denote the separable closure and the algebraic closure of k, respectively. For every prime p, F_p will be the field with p elements, $\mathbf{Z}_p$ will denote the ring of integers of Q_p, and Q will denote the field of rational numbers.

I wish to acknowledge my indebtedness to Professor H. Furstenberg for several useful conversations and especially for an idea which led me to Theorem 4.

DEFINITION. Let k be a field and let t be a transcendental element over k. A separable polynomial $f \in k(t)[Z]$ is said to be "stable over k" if the Galois group, $\mathcal{G}(f, k(t))$, of f over $k(t)$ is isomorphic to the Galois group, $\mathcal{G}(f, \tilde{k}(t))$, of f over $\tilde{k}(t)$.

It is clear that if $f(t, Z)$ is stable over k then $\mathcal{G}(f, k(t)) \cong \mathcal{G}(f, l(t))$ for every algebraic extension l of k. Furthermore, we have the following lemma:

LEMMA 1. *If $f(t, Z)$ is a stable polynomial over a field k and if l is any extension of k over which t is transcendental then $\mathcal{G}(f, k(t)) \cong \mathcal{G}(f, l(t))$.*

Proof. Let $l_0 = l \cap \tilde{k}$. Then l is a primary extension of l_0 (see Lang [5, p. 60]). Since t is transcendental over l, l is linearly disjoint from $l_0(t)$ over l_0. (See Lang [5, p. 52, Proposition 3]), hence l is free from $l_0(t)$ over l_0 (See Lang [5, p. 52, Propositon 2)], hence l is free from $l_0(t)_s$. Moreover, $l_0(t)_s$ is a separable extension of l_0, hence, according to Lang [5, p. 61, Theorem 6], l and $l_0(t)_s$ are linearly disjoint over l_0. Hence, according to Lang [5, p. 50, Proposition 1], $l(t)$ and $l_0(t)_s$ are linearly disjoint over $l_0(t)$. Let now L be the splitting field of $f(t, Z)$ over $l_0(t)$. Then $L \cap l(t) = l_0(t)$, hence $\mathcal{G}(f, l(t)) \cong \mathcal{G}(L/l_0(t)) = \mathcal{G}(f, l_0(t))$. Since l_0 is an algebraic extension of k we have $\mathcal{G}(f, l_0(t)) \cong \mathcal{G}(f, k(t))$. Hence $\mathcal{G}(f, l(t)) \cong \mathcal{G}(f, k(t))$.

Q.E.D.

THEOREM 2. *For every finite group G there exists a finite set A of primes such that for every prime $p \notin A$ there exists a separable polynomial $f \in \tilde{F}_p[t, Z]$ for which $\mathcal{G}(f, \tilde{F}_p(t)) \cong G$ (t is transcendental over F_p).*

Also, there exists a set of primes, of positive Dirichlet density, such that for every $p \in S$ there exists a polynomial $f \in \mathbf{Z}_p[t, Z]$ which is stable over Q_p and for which $\mathcal{G}(f, Q_p(t)) \cong G$; moreover, the reduction of f modulo p is stable over F_p and its Galois group over $F_p(t)$ is again isomorphic to G.

Proof. Let G be a finite group. According to Douady's theorem, G is realizable over $\tilde{Q}(t)$. We can, therefore, choose an irreducible polynomial $f \in \tilde{Q}[t, Z]$ which is monic as a polynomial in Z, such that $\mathcal{G}(f, \tilde{Q}(t)) \cong G$. Let $z_1, \ldots, z_n$ be the roots of $f(t, Z)$ in $\widetilde{Q(t)}$. Let $y_1, \ldots, y_n$ be n different letters and denote by S_n the symmetric group of all permutations of $(y) = (y_1, \ldots, y_n)$. Consider G as a subgroup of S_n. Build the formal sum $\theta = z_1 y_1 + \cdots + z_n y_n$. For every $\gamma \in S_n$ put $\gamma\theta = z_1 \gamma y_1 + \cdots + z_n \gamma y_n$. Put also

$$h(y, X) = \prod_{\gamma \in S_n} (X - \gamma\theta).$$

h is a polynomial with coefficients in $\tilde{Q}[t]$ and as a polynomial in X it is

monic. Let $h = h_1 \cdots h_r$ be a decomposition of h over $\tilde{Q}[t]$. It is also a decomposition over $\tilde{Q}(t)$. Thus, each of the factors h_ρ is irreducible over $\tilde{Q}$ as a polynomial in (t, y, X). According to a criterion which can be found in Van-der-Warden [8, p. 189, Section 61], we have

$$\gamma \in G \Leftrightarrow \gamma h_1 = h_1 . \tag{1}$$

Let p be a prime and let π be any place of $\tilde{Q}$ which extends p. For every polynomial g which is defined over $\tilde{Q}$ we denote by g^π its image under π. Since (1) is an elementary statement over $\tilde{Q}$, a lemma of *Ax* [1, p. 169, Lemma 4] implies that there exists a finite set A of primes such that for every $p \notin A$ and for every place π which extends p, the polynomials $f^\pi, h_1^\pi, \ldots, h_r^\pi$ are defined and irreducible over $\tilde{F}_p$; f^π is separable and $\gamma \in G \Leftrightarrow \gamma h_1^\pi = h_1^\pi$. (This results also from Shimura [7, Section 6] rather than from *Ax*'s lemma). Since $h^\pi = h_1^\pi \cdots h_r^\pi$ Van-der-Warden's criterion implies that $\mathcal{G}(f^\pi, \tilde{F}_p(t)) \cong G$.

This proves the first part of the theorem. In order to prove the second one we take a finite Galois extension k of Q over which $f, h_1, \ldots, h_r$ are defined. Since they are also irreducible over k, according to Van-der-Warden's criterion, $\mathcal{G}(f, k(t)) \cong G$, and thus f is stable over k. According to Čebotarev density theorem. (See, e.g., Cassels and Fröhlich [2, p. 227]) there exists a set of primes, S', of positive Dirichlet density, such that for every prime $p \in S'$ the decomposition field of every prime ideal of k which lies over p, is k itself. (This, in fact, is the set of all primes p which are unramified in k, for which the Artin symbol $((k/Q)/p)$ is the identity of $\mathcal{G}(k/Q)$. The density of this set is $1/[k : Q]$). Put $S = S' - A$; For every $p \in S$ k can be imbedded in Q_p and hence f can be considered as being defined over $\mathbf{Z}_p$. According to Lemma 1, $\mathcal{G}(f, Q_p(t)) \cong G$ and f is stable over Q_p. Moreover, for every place π which extends p, $f^\pi, h_1^\pi, \ldots, h_r^\pi$ are already defined over F_p. Since they are clearly irreducible over F_p, then according to Van-der-Warden's criterion, we have $\mathcal{G}(f^\pi, F_p(t)) \cong G$. This implies that f^π is stable over F_p. Q.E.D.

Since every separable polynomial $f(t, Z) \in \tilde{F}_p[t, Z]$ is clearly stable over $\tilde{F}_p$, we have from Lemma 1 and Theorem 2 the following corollary:

COROLLARY 3. *For every finite group G there exists a finite set A of primes such that for every $p \notin A$ and for every field k which contains $\tilde{F}_p$, G is realizable over $k(t)$, where t is a transcendental element over k.*

Also, there exists a set S of primes of positive Dirichlet density, such that for every $p \in S$ and for every field k which is either of characteristic p or contains Q_p, G is realizable over $k(t)$.

DEFINITION. An imbedding problem is a diagram of the form

$$\begin{array}{ccccccc} 1 \to H & \xrightarrow{\kappa} & G & \xrightarrow{\pi} & G' \to 1 \\ & & & & \downarrow \phi' \\ & & & & \mathcal{G}(L/K) \end{array} \tag{2}$$

for which the upper row is a short exact sequence of finite groups, K is a field, L is a Galois extension of K and ϕ' is an isomorphism. Let n be a positive integer. We say that (2) is an n-bounded imbedding problem if the order of G is $\leqslant n$. We say that "the imbedding problem (2) splits completely" if G is the cartesian product of κH and the image of G' in G by a homomorphism $\nu : G' \to G$ for which $\pi \circ \nu = 1$. We say that "the imbedding problem (2) is solvable" if there exists a Galois extension M of K which contains L and if there exists an isomorphism $\phi : G \to \mathcal{G}(M/K)$ such that the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\kappa} & G & \xrightarrow{\pi} & G' & \longrightarrow & 1 \\ & & & & \downarrow \phi & & \downarrow \phi' & & \\ 1 & \to & \mathcal{G}(M/L) & \to & \mathcal{G}(M/K) & \to & \mathcal{G}(L/K) & \to & 1, \end{array}$$

in which the mappings in the lower row are the natural ones, commutes.

THEOREM 4. *For every positive integers d, n there exists a finite set A of primes such that if p is a prime not in A, k an extension of $\tilde{F}_p$, t a transcendental element over k and K an extension of $k(t)$ of degree $\leqslant d$, then every n-bounded problem of the form* (2) *which splits completely is solvable.*

Also there exists a set S of primes, of positive Dirichlet density, such that if $p \in S$, k is either a field of characteristic p or a field which contains Q_p, t is a transcendental element over k, and K is an extension of $k(t)$ of degree $\leqslant d$, then every n-bounded problem of the form (2) *which splits completely is solvable.*

Proof. We prove the first part of the theorem. The proof of the second part is analogous.

Since there exists only a finite number of finite groups whose order $\leqslant n$, we can assume, without loss of generality that the upper row in (2) is given. Let l be the order of G'. From Corollary 3 it follows that there exists a finite set A of primes such that if p is a prime not in A, k is an extension of $\tilde{F}_p$, and t is transcendental over k, then the cartesian product of H with itself $2^{dl} + 1$ times is realizable over $k(t)$. Take such p, k and t. We obtain for them $2^{dl} + 1$ Galois extensions N_i of $k(t)$ such that $\mathcal{G}(N_i/k(t)) \cong H$ and $N_i \cap N_j = k(t)$ for every $i \neq j$. Now let K be an extension of $k(t)$ of degree d and let L be a Galois extension of K such that $\mathcal{G}(L/K) \cong G'$. Denote by L'

the maximal separable extension of $k(t)$ contained in L. Its degree is certainly $\leqslant dl$. Hence the number of its subextensions does not exceed 2^{dl}. (This follows by analyzing the proof that a simple extension has only finitely many subextensions, as appears, for example, in Lang [6, p. 185, Theorem 14]). Therefore there exist $i \neq j$ such that $N_i \cap L' = N_j \cap L'$. But then we have $N_i \cap L' = k(t)$. This implies that also $N_i \cap L = k(t)$. So, if we put $M = N_i \cap L$ we have $\mathcal{G}(M/L) \cong H$, and the short exact sequence

$$1 \to \mathcal{G}(M/L) \to \mathcal{G}(M/K) \to \mathcal{G}(L/K) \to 1$$

splits completely.

Let ψ be an isomorphism of H onto $\mathcal{G}(M/L)$. Using ϕ' and ψ we can easily build an isomorphism $\phi : G \to \mathcal{G}(M/K)$ such that the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H & \xrightarrow{\kappa} & G & \xrightarrow{\pi} & G' & \longrightarrow & 1 \\ & & \psi\downarrow & & \phi\downarrow & & \phi'\downarrow & & \\ 1 & \to & \mathcal{G}(M/L) & \to & \mathcal{G}(M/K) & \to & \mathcal{G}(L/K) & \to & 1 \end{array}$$

commutes. Thus the problem (2) is solvable for every K and L as specified above. Q.E.D.

We note that the first part of Theorems 2 and 4 follows also from well-known results of Grothendieck and it was brought here only for the sake of completeness.

References

1. J. Ax, Solving diophantine problems modulo every prime, *Ann. of Math.* **85** (1967), 161–183.
2. J. W. S. Cassels and A. Fröhlich, "Algebraic number theory," Academic Press, New York, 1962.
3. A. Douady, Determination d'un groupe de Galois, *C. R. Acad. Sci. Paris* **258** (1964), 5305–5308.
4. M. Jarden, Elementary statements over large algebraic fields, *Transactions Amer. Math. Soc.* **163** (1972), 67–91.
5. S. Lang, Introduction to algebraic geometry, Interscience, New York, 1958.
6. S. Lang, "Algebra," Addison-Wesley, Reading, Massachusetts, 1965.
7. G. Shimura, Reduction of algebraic varieties with respect to a discrete valuation of the basic field, *Amer. J. Math.* **77** (1955), 134–176.
8. B. L. van der Warden, "Modern Algebra," Vol. I, 1937.