Ann. Sci. Math. Québec **32** (2008), no 2, 171–174

THE GALOIS RELATIONS $x_1 = x_2 + x_3$ AND $x_1 = x_2\,x_3$ FOR CERTAIN SOLVABLE GROUPS

KURT GIRSTMAIR

Dedicated to professor John Labute on the occasion of his 70th birthday.

RÉSUMÉ. Soit G un groupe fini, réalisé comme groupe de Galois sur un corps de nombres K. Il a été conjecturé qu'il existe un polynôme irréductible $f \in K[X]$, de groupe de Galois G et dont les racines vérifient la relation $x_1 = x_2 + x_3$ (ou $x_1 = x_2x_3$), avec une numérotation appropriée des racines, dès que $|G| \equiv 0 \pmod 6$. Nous prouvons le résultat suivant qui va dans le sens de cette conjecture : s'il existe un sous-groupe résoluble H de G tel que $|H| \equiv 0 \pmod 6$, ces relations ont lieu pour un certain polynôme f de groupe de Galois G, dont l'action est regulière sur les racines de f.

ABSTRACT. Let G be a finite group that occurs as a Galois group over an algebraic number field K. It has been conjectured that there exists an irreducible polynomial $f \in K[X]$ with Galois group G that permits the relation $x_1 = x_2 + x_3$ (or $x_1 = x_2x_3$) between its (suitably numbered) roots, whenever $|G| \equiv 0 \pmod 6$. Here we support this conjecture by the following result: If G has a solvable subgroup H, with $|H| \equiv 0 \pmod 6$, these relations are possible for a polynomial f with Galois group G, where G acts regularly on the roots of f.

1. Introduction and main result

In what follows, let K be a field of characteristic 0. The question whether an irreducible polynomial $f \in K[X]$ (in one indeterminate) may afford a relation like $x_1 = x_2 + x_3$ or $x_1 = x_2\,x_3$ reportedly goes back to J. Browkin and A. Schinzel. Since the mid-nineties it was studied in a number of papers; see [2], [1], [3], [4] and [7] (in chronological order). This question is closely connected with the Galois group G of f, more precisely, with the action of G on the roots $x_1, \ldots, x_n$ of f. The most hopeful setting for the existence of relations of this kind is given when G acts *regularly* on these roots (so each root is fixed only by $1 \in G$, which is the same as saying $n = |G|$). Indeed, for no other kind of action it is possible to have as many relations as for the regular one. Hence this will be our main case here.

In [3] it was shown that $x_1 = x_2 + x_3$ is possible for abelian groups G if, and only if, $|G| \equiv 0 \pmod 6$ (note that G acts faithfully on $x_1, \ldots, x_n$, and so "abelian" automatically implies "regular"). It was also shown in [3] that the theories of additive

Reçu le 16 mai 2008 et, sous forme définitive, le 19 octobre 2008.

and multiplicative relations are basically identical. This means that $x_1 = x_2 + x_3$ is always possible (more or less) when $x_1 = x_2\,x_3$ is possible, and conversely. However, the case of this multiplicative relation (for abelian groups G) had been settled earlier; see [2].

In [5] we proved that both relations are possible for regular actions of arbitrary simple nonabelian groups G. Of these groups, only the Suzuki groups have an order not divisible by 6. Since abelian and simple nonabelian groups represent, in some sense, the extreme cases, one is lead to the conjecture that these relations may occur whenever G acts regularly and $|G| \equiv 0 \pmod 6$ (a conjecture raised by F. Lalande and others).

In this note we prove another result that supports this conjecture. In contrast to the theorems of [5], its proof makes no use of the classification of finite simple groups but only of classical methods of group theory.

Theorem 1. *In the above setting, let G be a finite group that contains a solvable subgroup H with $|H| \equiv 0 \pmod 6$. Suppose, further, that G occurs as a Galois group over K.*

(a) *There is an irreducible polynomial $f \in K[X]$ with Galois group G such that G acts regularly on the roots $x_1, \ldots, x_n$ of f and $x_1 = x_2 + x_3$ (when the roots are suitably numbered).*

(b) *Assume, in addition, that there is a place $\mathfrak{p}$ of K that splits completely in a Galois extension L of K with $G = \mathrm{Gal}(L/K)$. Then there is an irreducible polynomial $f \in K[X]$ with splitting field L such that G acts regularly on the roots $x_1, \ldots, x_n$ of f and $x_1 = x_2\,x_3$ (suitably numbered, again).*

We briefly discuss some natural questions connected with Theorem 1. The condition $|H| \equiv 0 \pmod 6$ is not necessary for our relations to hold, as the example $G = \mathrm{ASL}(1, 11)$, $|G| = 55$, shows. Here both relations are possible by Theorem 1 of [4], since $1 \equiv 3^2 + 6^2 \pmod{11}$. On the other hand, none of $|H| \equiv 0 \pmod 2$ and $|H| \equiv 0 \pmod 3$ is sufficient because these relations are impossible for abelian groups G with $|G| \not\equiv 0 \pmod 6$.

What about the case when G does not act regularly? For a necessary condition that covers certain cases, see [1]. Conversely, the Corollary to Proposition 10 in [3] says that both relations are possible if $G = FJ$, where F is a cyclic normal subgroup of G, $|F| \equiv 0 \pmod 6$, J is an arbitrary group with $F \cap J = 1$, and G acts faithfully on G/J (here the group J will be the stabilizer of one of the roots of the polynomial $f \in K[X]$). An example of this kind is the dihedral group G of order 12, with $F = C_6$ and $J = C_2$ (cyclic groups of respective order). In this example, however, G acts imprimitively on the roots of f, as in all other examples known to us. It would be interesting to know whether there is a Galois group G acting primitively on $x_1, \ldots, x_n$ and admitting a three-term relation like $x_1 = x_2 + x_3$ or $x_1 + x_2 + x_3 = 0$ ($n > 3$ in the last-mentioned case).

2. Proof of the main result

By Proposition 1 of [4], it suffices to show that there is a subgroup H' of H and elements $s, t \in H' \setminus \{1\}$, with $s \neq t$, such that $\alpha = 1 - s - t$ is an admissible element of the rational group ring $\mathbb{Q}[H']$; here *admissible* means that α annihilates an element $\tau \in \mathbb{Q}[H']$ whose stabilizer $H'_\tau = \{u \in H' : u\tau = \tau\}$ equals $\{1\}$ (for the multiplicative case (b), see also Propositions 4 and 5 of [3]). A possible choice for H' is the cyclic group C_6, the symmetric group S_3, or the alternating group A_4. For these three groups admissible elements of the desired shape do exist; see [4], Corollary to Proposition 1, and references. So our proof comes down to showing that each solvable group H with $|H| \equiv 0 \pmod 6$ contains one of these groups (up to isomorphy, of course).

Since H is solvable, it contains a $(2,3)$-Hall group H_1; see [6], Kap. VI, Hauptsatz 1.8. In particular, $|H_1|$ is divisible only by 2 and 3, and $|H_1| \equiv 0 \pmod 6$. Let F be a minimal normal subgroup of H_1. Since H_1 is solvable, F is an elementary abelian p-group; see [6], Kap. I, Satz 9.13. But this requires either $F \cong \mathbb{F}_2^m$ or $F \cong \mathbb{F}_3^m$, where $\mathbb{F}_p$ is the field of p elements, and $m \geq 1$. We write $F = \mathbb{F}_p^m$ henceforth.

Case 1. Suppose $F = \mathbb{F}_2^m$. Put $T = \langle t \rangle$, where $t \in H_1$ has order 3. As F is a normal subgroup of H_1, the group T acts on F by conjugation, in particular, as an automorphism group of F. Since the automorphism group of $F = \mathbb{F}_2^m$ is the linear group $\mathrm{GL}(\mathbb{F}_2^m)$, we obtain a representation

$$\rho : T \to \mathrm{GL}(\mathbb{F}_2^m).$$

By means of ρ, the $\mathbb{F}_2$-vector space $\mathbb{F}_2^m$ becomes a module over the (commutative) group ring $\mathbb{F}_2[T]$. Because the characteristic of $\mathbb{F}_2$ does not divide the group order $|T| = 3$, this module is semisimple. Hence it must contain a simple $\mathbb{F}_2[T]$-submodule V. However, all possible simple $\mathbb{F}_2[T]$-modules can be read from the decomposition

$$\mathbb{F}_2[T] = V_0 \oplus V_1,$$

where

$$V_0 = \mathbb{F}_2(1 + t + t^2)$$

is the trivial submodule of $\mathbb{F}_2[T]$ and

$$V_1 = \mathbb{F}_2(1 + t) + \mathbb{F}_2(1 + t^2)$$

has $\mathbb{F}_2$-dimension 2 (note that $t + t^2 = (1 + t) + (1 + t^2)$; further, $1 + t$ and $1 + t^2$ annihilate V_0). If V is isomorphic to V_0, T acts trivially on the subgroup V of order 2 of F, hence VT is isomorphic to C_6. If V is isomorphic to V_1, the cyclic group T acts on the subgroup $V \cong \mathbb{F}_2^2$ of F in a nontrivial way, hence $VT = TV$ is isomorphic to A_4.

Case 2. Suppose $F = \mathbb{F}_3^m$. Here we take an element $s \in H_1$ of order 2 and put $S = \langle s \rangle$. Then $\mathbb{F}_3^m$ becomes a semisimple $\mathbb{F}_3[S]$-module by the argument of Case 1. Let W be a simple submodule of $\mathbb{F}_3^m$. If W is trivial (that is, isomorphic to $\mathbb{F}_3(1 + s)$), the group WS is isomorphic to C_6. In the remaining case we have $W \cong \mathbb{F}_3(1 - s)$, so S acts on the group W of three elements nontrivially, and $WS = SW \cong S_3$. $\square$

REFERENCES

[1] J. D. Dixon, *Polynomials with nontrivial relations between their roots*, Acta Arith. **82** (1997), 293–302.

[2] M. Drmota, M. Skałba, *Relations between polynomial roots*, Acta Arith. **71** (1995), no. 1, 65–77.

[3] K. Girstmair, *Linear relations between roots of polynomials*, Acta Arith. **89** (1999), no. 1, 53–96.

[4] K. Girstmair, *The Galois relation $x_1 = x_2 + x_3$ and Fermat over finite fields*, Acta Arith. **124** (2006), no. 4, 357–370.

[5] K. Girstmair, *The Galois relation $x_1 = x_2 + x_3$ for finite simple groups*, Acta Arith. **127** (2007), no. 3, 301–303.

[6] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band **134**, Springer-Verlag, Berlin-New York, 1967, xii+793 pp.

[7] F. Lalande, *La relation linéaire a=b+c+… +t entre les racines d'un polynôme*, J. Théor. Nombres Bordeaux **19** (2007), no. 2, 473–484.

K. GIRSTMAIR, INSTITUT FÜR MATHEMATIK, U. INNSBRUCK TECHNIKERSTR. 13/7, A-6020 INNSBRUCK, AUSTRIA
Kurt.Girstmair@uibk.ac.at