ACTA ARITHMETICA
127.3 (2007)

The Galois relation $x_1 = x_2 + x_3$ for finite simple groups

by

Kurt Girstmair (Innsbruck)

In this note we prove the following theorem (which occurred in [4] as a conjecture):

Theorem 1. *Let K be a field of characteristic* 0 *and L a finite Galois extension of K such that $G = \mathrm{Gal}(L/K)$ is a nonabelian simple group. Then there is an element $x \in L$ such that*

$$L = K(x) \quad \textit{and} \quad x = s(x) + t(x) \quad \textit{for some } s, t \in G \smallsetminus \{1\},\ s \neq t.$$

In other words, every polynomial f over K whose Galois group is nonabelian and simple has a *Galois resolvent* g such that $x_1 = x_2 + x_3$ holds for suitably numbered zeros x_1, x_2, x_3 of g.

Proof of Theorem 1. By Proposition 1 of [4], it suffices to show that G contains a subgroup G' such that the group ring $K[G']$ of G' contains an admissible element $1 - s - t$, $s, t \in G' \smallsetminus \{1\}$ (which means that there is a $\tau \in K[G']$ such that $(1 - s - t)\tau = 0$ and $\{u \in G' : u\tau = \tau\} = \{1\}$). Now, it has been shown in [1] that the group G contains a *minimal simple* group G' in the sense of [7, Section 2]. However, such a group G' is either a simple *linear* group $\mathrm{PSL}(n, q)$ or a Suzuki group $\mathrm{Sz}(2^{2n+1})$ ([7, Corollary 1]). But Proposition 2 of [4] says that the group ring of every simple linear group contains an admissible element of the desired shape. The same holds for the Suzuki groups ([4, last paragraph]). ∎

Remarks. 1. We only recently learned that finite nonabelian simple groups *actually* contain minimal simple groups. This is by no means obvious. Quite the reverse, the proof of this fact uses the classification of finite simple groups (see [1]). On the other hand, Proposition 2 of [4] settles an important special case of Theorem 1 in a rather easy way. Hence we think that the proof of this proposition still has some value.

2000 *Mathematics Subject Classification*: 12F10, 12E05.

2. The said proof depends on subgroups $\mathrm{AGL}(1,q)$ or $\mathrm{ASL}(1,q)$ of finite linear groups $\mathrm{PSL}(n,q)$, because of the fact that the group rings of these subgroups contain admissible elements of the desired type. Accordingly, the above proof of Theorem 1 involves an *infinite series* of groups $\mathrm{AGL}(1,q)$. In the light of [1], however, this proof could be based upon only *three* of these groups, namely, $S_3 = \mathrm{AGL}(1,3)$, $A_4 = \mathrm{AGL}(1,4)$, and $\mathrm{AGL}(1,5)$. Indeed, a minimal simple group that is linear contains A_4, with the exception of the groups $\mathrm{PSL}(2,2^p)$, p an odd prime, which contain S_3, however (see [5, p. 213] and [2, p. 13]). Each Suzuki group contains the group $\mathrm{AGL}(1,5)$ (as follows from [6, p. 190]).

In [4] we did not mention the *multiplicative* analogue $x_1 = x_2x_3$ of the relation $x_1 = x_2 + x_3$. This is regrettable inasmuch as our previous paper [3] shows that the theories of additive and multiplicative relations are almost identical. Accordingly, we note

THEOREM 2. *Let K be a field of characteristic 0 and L a finite Galois extension of K such that $G = \mathrm{Gal}(L/K)$ is a nonabelian simple group. Assume, further, that there is a place $\mathfrak{p}$ of K that splits completely in L. Then there is an element $y \in L$ such that*

$$L = K(y) \quad \text{and} \quad y = s(y)t(y) \quad \text{for some } s,t \in G \setminus \{1\},\ s \neq t.$$

Proof. The main issue is the fact that the admissible element $1 - s - t$ in question lies in the *rational* group ring $\mathbb{Q}[G]$ of G, not only in $K[G]$. Therefore, Propositions 4 and 5 of [3] yield the result. ∎

REMARK. Theorem 2 applies to finite Galois extensions of arbitrary *algebraic number fields K* (with appropriate group, of course), since the assumption about the place $\mathfrak{p}$ holds in this case.

The author gratefully acknowledges the support by the Austrian Science Fund (FWF Project P16641-N12).

References

[1] M. J. J. Barry and M. B. Ward, *Simple groups contain minimal simple groups*, Publ. Mat. 41 (1997), 411–415.

[2] J. H. Conway *et al.*, *Atlas of Finite Groups*, Clarendon Press, Oxford, 1985.

[3] K. Girstmair, *Linear relations between roots of polynomials*, Acta Arith. 89 (1999), 53–96.

[4] —, *The Galois relation $x_1 = x_2 + x_3$ and Fermat over finite fields*, ibid. 124 (2006), 357–370.

[5] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967.

[6] B. Huppert and N. Blackburn, *Finite Groups III*, Springer, Berlin, 1982.

[7] J. G. Thompson, *Nonsolvable finite groups all of whose local subgroups are solvable*, Bull. Amer. Math. Soc. 74 (1968), 383–437.

Institut für Mathematik
Universität Innsbruck
Technikerstr. 13
A-6020 Innsbruck, Austria
E-mail: Kurt.Girstmair@uibk.ac.at

Received on 1.12.2006 (5336)