JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Jack SONN

Two remarks on the inverse Galois problem for intersective polynomials

Tome 21, n° 2 (2009), p. 435-437.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_2_435_0>

Journal de Théorie des Nombres de Bordeaux **21** (2009), 435-437

Two remarks on the inverse Galois problem for intersective polynomials

par Jack SONN

Résumé. Un polynôme (unitaire) $f(x) \in \mathbb{Z}[x]$ est dit *intersectif* si la congruence $f(x) \equiv 0 \bmod m$ a des solutions pour tout entier positif m. On dit que $f(x)$ est *non-trivialement intersectif* s'il est intersectif et n'a pas de racine rationnelle. L'auteur a prouvé que tout groupe fini G, résoluble non cyclique, peut être réalisé comme groupe de Galois sur $\mathbb{Q}$ d'un polynôme non-trivialement intersectif (non cyclique est une condition nécessaire). Notre premiere remarque est l'observation que le résultat correspondant pour les groupes non-résolubles G se ramène au problème de Galois inverse ordinaire pour G sur $\mathbb{Q}$. La seconde remarque concerne la rareté d'exemples explicites de polynômes non-trivialement intersectifs de groupe de Galois donné, et nous donnons le premier exemple connu pour le groupe dihédral d'ordre dix.

Abstract. A (monic) polynomial $f(x) \in \mathbb{Z}[x]$ is called *intersective* if the congruence $f(x) \equiv 0 \bmod m$ has a solution for all positive integers m. Call $f(x)$ *nontrivially intersective* if it is intersective and has no rational root. It was proved by the author that every finite noncyclic solvable group G can be realized as the Galois group over $\mathbb{Q}$ of a nontrivially intersective polynomial (noncyclic is a necessary condition). Our first remark is the observation that the corresponding result for nonsolvable G reduces to the ordinary inverse Galois problem for G over $\mathbb{Q}$. The second remark has to do with the scarcity of explicit examples of nontrivial intersective polynomials with given Galois group, and gives the first known example for the dihedral group of order ten.

A (monic) polynomial $f(x) \in \mathbb{Z}[x]$ is called *intersective* if the congruence $f(x) \equiv 0 \bmod m$ has a solution for all positive integers m. Call $f(x)$ *nontrivially intersective* if it is intersective and has no rational root. It was proved by the author that every finite noncyclic solvable group G can be realized as the Galois group over $\mathbb{Q}$ of a nontrivially intersective polynomial (noncyclic is a necessary condition) [4, Thm 2.2]. This note makes the observation that the corresponding result for nonsolvable G reduces to the ordinary inverse Galois problem for G over $\mathbb{Q}$.

Proposition. *Let G be a finite nonsolvable group. The following are equivalent:*

(1) G is realizable as the Galois group of a nontrivially intersective polynomial over $\mathbb{Q}$

(2) G is realizable as a Galois group over $\mathbb{Q}$.

Proof. (1)$\Longrightarrow$ (2) is trivial. Assume (2). As noted in [4], a monic polynomial $f(x) \in \mathbb{Z}[x]$ has a root mod n for all n if and only if $f(x)$ has a root in $\mathbb{Q}_p$ for all (finite) primes p. Let $G = G(K/\mathbb{Q})$. By [4, Prop. 2.1], the following are equivalent:

(i) K is the splitting field of a product $f = g_1 \cdots g_m$ of m irreducible polynomials of degree greater than 1 in $\mathbb{Q}[x]$ and f has a root in $\mathbb{Q}_p$ for all primes p.

(ii) G is the union of the conjugates of m proper subgroups $A_1, ..., A_m$, the intersection of all these conjugates is trivial, and for all primes $\mathfrak{p}$ of K, the decomposition group $G(\mathfrak{p})$ is contained in a conjugate of some A_i.

It therefore suffices to show that G has such a covering $A_1, ..., A_m$. Since any decomposition group $G(\mathfrak{p})$ is necessarily solvable, hence a proper subgroup of G, we can take for example $A_1, ..., A_m$ to be the set of all proper subgroups of G (obviously not the most economical choice). Clearly their intersection is trivial, since for example a nonsolvable group has elements of prime order for at least two distinct primes. The result then follows. □

An Example. In [2], (see also [1]), the polynomials $(x^r - 2)\Phi_r(x)$, $r \geq 3$ a prime ($\Phi_r(x)$ is the rth cyclotomic polynomial), with Galois groups the Frobenius groups of order $r(r-1)$, are given as examples of polynomials with no rational roots and roots mod p for all p. Examples of nontrivial intersective polynomials are still rare. For instance the above examples do not include the dihedral group D_{10} of order ten, which, like the above examples, is a Frobenius group and in particular is the union of conjugates of two proper subgroups, and where the desired polynomial should be a product of two irreducible factors. The results in [4] are purely existence theorems and do not give explicit polynomials. We now give an example of a nontrivial intersective polynomial with Galois group D_{10} which is a product of two irreducible factors.

In [3, p. 171], the polynomial $f(x) = x^5 + x^4 - 5x^3 - 4x^2 + 3x + 1$ is given as an example of a polynomial with Galois group D_{10} over $\mathbb{Q}$, with all real roots. Its discriminant is 401^2 (401 is a prime) hence the quadratic subfield of its splitting field is $\mathbb{Q}(\sqrt{401})$. We claim that all decomposition groups are cyclic. Since $401 \equiv 1 \pmod 8$, the prime 2 splits completely in $\mathbb{Q}(\sqrt{401})$, so the only ramified prime in $\mathbb{Q}(\sqrt{401})$ is 401. From the structure of D_{10} we see that the decomposition group at 401 is cyclic (of order 2). Secondly, since the prime 2 splits completely in $\mathbb{Q}(\sqrt{401})$, the decomposition group at 2 is cyclic as well. In fact, f is irreducible mod 2, so 2 is unramified with decomposition group cyclic of order 5. All other primes are unramified, so all other decomposition groups are also cyclic. We may now apply condition (ii) in the proof of the proposition above, with A_1 the subgroup of order 5 and A_2 of order 2. It follows that $f(x)(x^2 - 401)$ has a root in $\mathbb{Q}_p$ for all p.

References

[1] D. Berend and Y. Bilu, *Polynomials with roots modulo every integer*. Proc. AMS **124** (1996), 1663–1671.

[2] R. Brandl, *Integer polynomials with roots mod p for all primes p*. J. Alg. **240** (2001), 822–835.

[3] C. Jensen, A. Ledet, and N. Yui, *Generic Polynomials*. Cambridge Univ. Press, Cambridge-New-York, 2002.

[4] J. Sonn, *Polynomials with roots in $\mathbb{Q}_p$ for all p*. Proc. AMS **136** (2008), 1955–1960.

Jack Sonn
Department of Mathematics
Faculty of Mathematics
Technion–Israel Institute of Technology
Haifa, Israel
E-mail: sonn@tx.technion.ac.il