PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 6, June 2008, Pages 1955–1960
S 0002-9939(08)09155-7
Article electronically published on February 12, 2008

POLYNOMIALS WITH ROOTS IN $\mathbb{Q}_p$ FOR ALL p

JACK SONN

(Communicated by Ken Ono)

Abstract. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ with no rational roots but with roots in $\mathbb{Q}_p$ for all p, or equivalently, with roots mod n for all n. It is known that $f(x)$ cannot be irreducible but can be a product of two or more irreducible polynomials, and that if $f(x)$ is a product of $m > 1$ irreducible polynomials, then its Galois group must be a union of conjugates of m proper subgroups. We prove that for any $m > 1$, every finite solvable group that is a union of conjugates of m proper subgroups (where all these conjugates have trivial intersection) occurs as the Galois group of such a polynomial, and that the same result (with $m = 2$) holds for all Frobenius groups. It is also observed that every nonsolvable Frobenius group is realizable as the Galois group of a geometric, i.e. regular, extension of $\mathbb{Q}(t)$.

1. Introduction

Let $f(x)$ be a monic polynomial with rational integer coefficients. Suppose f has no rational roots but has a root in $\mathbb{Q}_p$ for all p, or equivalently, has a root mod n for all positive integers n. It has been observed [BeBi], [Br] that f cannot be irreducible (even under the slightly weaker assumption that f has a root mod p for all prime numbers p), and that if f is a product of $m > 1$ irreducible polynomials, then its Galois group must be a union of conjugates of m proper subgroups.[1] Indeed, if f is irreducible, let α be a root of f, $F = \mathbb{Q}(\alpha)$, K the splitting field of f over $\mathbb{Q}$, and G the Galois group $G(K/\mathbb{Q})$. Let p be a prime not dividing the discriminant disc(f) of f. f has a root mod p implies that for some prime $\mathfrak{p}$ of K dividing p, the decomposition group $G(\mathfrak{p})$ of $\mathfrak{p}$ is contained in $G(K/F)$, or equivalently, for any prime $\mathfrak{p}$ of K dividing p, there exists a root β of f such that $G(\mathfrak{p}) \subseteq G(K/\mathbb{Q}(\beta))$. By Chebotarev's density theorem, $G = \bigcup_{\mathfrak{p}\nmid \mathrm{disc}(f)} G(\mathfrak{p})$. But then

$$\bigcup_{\mathfrak{p}\nmid \mathrm{disc}(f)} G(\mathfrak{p}) \subseteq \bigcup_{f(\beta)=0} G(K/\mathbb{Q}(\beta))$$

cannot equal G since a union of conjugates of a proper subgroup of a finite group cannot equal the whole group. Thus f cannot be irreducible. By a similar argument, if f is a product $g_1 \cdots g_m$ of m irreducible polynomials in $\mathbb{Z}[x]$ (of degree greater than 1) with splitting field K and Galois group G, then G is a union of conjugates of m proper subgroups, namely $G(K/\mathbb{Q}(\alpha_i))$, where $g_i(\alpha_i) = 0$, $i = 1, ..., m$. Finite groups that are the union of conjugates of two proper subgroups are studied in [Br],

Received by the editors January 4, 2007, and, in revised form, March 8, 2007.
2000 *Mathematics Subject Classification.* Primary 11R32, 12F12.

[1] In [BeBi], an effective condition is given for checking if f has this property.

where it is proved among other things that if a group G has this property, and the two subgroups are nilpotent, then G is solvable. It is also proved in [BBH] that if the symmetric group S_n has this property, then $3 \leq n \leq 6$. In [Br] (see also [BeBi]), 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, and the inverse problem is raised: if G is a union of conjugates of two proper subgroups (one should also assume that the intersection of all these conjugates is trivial), then can G be realized as the Galois group of the product f of two irreducible nonlinear polynomials such that f has a root mod p for all p? The answer appears not to have been known even for the dihedral group of order ten. We will prove that every finite solvable group with the above property can be realized in this way, with f having a root in $\mathbb{Q}_p$ for all p. As it turns out, Shafarevich's realization of solvable groups already yields extensions with the required property (even for "m proper subgroups" and "m irreducible polynomials" instead of two). We will also prove the result for all nonsolvable Frobenius groups. On the other hand, the question seems to be open even for the symmetric group S_6, which as we mentioned above, is the union of conjugates of two proper subgroups. In connection with Frobenius groups, we observe that every nonsolvable Frobenius group is realizable as the Galois group of a geometric, i.e. regular, extension of $\mathbb{Q}(t)$, a fact that does not seem to have been pointed out before.

2. Roots in $\mathbb{Q}_p$ for all p

We begin with a characterization of Galois extensions which are splitting fields of polynomials that are products of m irreducible nonlinear polynomials in $\mathbb{Q}[x]$ and that have roots in $\mathbb{Q}_p$ for all p. Note that if $f \in \mathbb{Z}[x]$ has a root in $\mathbb{Q}_p$, then f has a root mod p.

Proposition 1. *Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group G. The following are equivalent:*

(1) 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.

(2) 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.

Proof. Assume first that (1) holds, i.e. K is the splitting field of a product $f = g_1 \cdots g_m$ of m irreducible polynomials of degree greater than 1 and f has a root in $\mathbb{Q}_p$ for all primes p. Let $\alpha_1, ..., \alpha_m$ be roots of $g_1, ..., g_m$ respectively in K and let $A_i := G(K/\mathbb{Q}(\alpha_i)), 1 \leq i \leq m$. Let p be a given prime number. By assumption f has a root in $\mathbb{Q}_p$; hence some g_i has a root in $\mathbb{Q}_p$. Then for some prime $\mathfrak{p}$ of K dividing p, the decomposition group $G(\mathfrak{p})$ is contained in A_i, or equivalently, for every prime $\mathfrak{p}$ of K dividing p, the decomposition group $G(\mathfrak{p})$ is contained in some conjugate $G(K/\mathbb{Q}(\alpha_i'))$ of A_i. We therefore conclude that if f has a root in $\mathbb{Q}_p$ for all p, then for all primes $\mathfrak{p}$ of K, the decomposition group $G(\mathfrak{p})$ is contained in a conjugate of some A_i. By Chebotarev's density theorem, every cyclic subgroup of G occurs as a decomposition group of some (unramified) prime $\mathfrak{p}$ of K; hence G is the union of the conjugates of $A_1, ..., A_m$. The intersection of all the conjugates of $A_1, ..., A_m$ is trivial because K is the splitting field of f. Thus (2) holds.

Conversely, assume (2), i.e. 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. Let $\alpha_1, ..., \alpha_m \in K$ such that $A_i = G(K/\mathbb{Q}(\alpha_i))$. Let $g_1, ..., g_m$ be the minimal polynomials of $\alpha_1, ..., \alpha_m$ resp. over $\mathbb{Q}$. Since the intersection of the conjugates of $A_1, ..., A_m$ is trivial, K is the splitting field of $f = g_1 \cdots g_m$ over $\mathbb{Q}$, and since $A_1, ..., A_m$ are proper subgroups of G, $g_1, ..., g_m$ have degrees greater than 1. Let p be a rational prime, $\mathfrak{p}$ a prime of K dividing p. By assumption the decomposition group $G(\mathfrak{p})$ of $\mathfrak{p}$ is contained in a conjugate of some A_i. Then g_i has a root in $\mathbb{Q}_p$. Thus our assumptions imply that f has a root in $\mathbb{Q}_p$ for all p. □

Note that (2) implies that G is necessarily noncyclic.

We now prove a realization theorem for solvable groups.

Theorem 2. *Let G be a finite solvable group which is the union of the conjugates of m proper subgroups, where the intersection of all these conjugates is trivial. Then there exists a polynomial $f(x)$ which is the product of m irreducible nonlinear polynomials in $\mathbb{Q}[x]$ with Galois group G and having a root in $\mathbb{Q}_p$ for all rational primes p. In particular* (since every noncyclic group is a union of (conjugates of) proper subgroups with trivial intersection)*, every noncyclic finite solvable group is realizable as the Galois group over $\mathbb{Q}$ of a polynomial $f(x) \in \mathbb{Q}[x]$ having no rational roots and having a root in $\mathbb{Q}_p$ for all rational primes p.*

Proof. The proof will follow easily from the observation that Shafarevich's realization of solvable groups as Galois groups over number fields yields an extension $K/\mathbb{Q}$ with all decomposition groups $G(\mathfrak{p})$ cyclic. Indeed, let G be a finite solvable group which is the union of the conjugates of m proper subgroups, and suppose $K/\mathbb{Q}$ is Galois with group G with all decomposition groups $G(\mathfrak{p})$ cyclic. Then every decomposition group is contained in a conjugate of some A_i, so by Proposition 1, we are done.

To verify the observation about Shafarevich's realization of solvable groups, we use the exposition of the proof of Shafarevich's theorem in [NSW]. The key result in the construction is [NSW, Theorem 9.5.11]. Let $\mathcal{F}(n)$ denote the free pro-$p-G$ operator group on n generators. G acts "freely" on $\mathcal{F}(n)$. There is a filtration $\mathcal{F}(n)^{(\nu)}$ ($\nu \in \mathbb{N} \times \mathbb{N}$) defined on $\mathcal{F}(n)$ which is a refinement of the descending p-central series, all of whose terms are G-invariant. (For the precise definition, see [NSW, pp. 481ff].) Now [NSW, Theorem 9.5.11] says that if K/k is any Galois extension of global fields with group G, then for any p, n, ν, the split embedding problem associated with the epimorphism $\mathcal{F}(n)/\mathcal{F}(n)^{(\nu)} \rtimes G \twoheadrightarrow G$ has a proper solution with solution field N_ν^n, such that (if $p \neq \mathrm{char}(K)$) all divisors of p, all infinite primes, and all primes of K which are ramified in K/k split completely in N_ν^n/K, and all primes $\mathfrak{p}$ of K which ramify in N_ν^n/K split completely in K/k, and the local extension $N_{\nu,\mathfrak{p}}^n/k_\mathfrak{p}$ is a totally ramified, hence cyclic, extension. In particular, if all decomposition groups in $G(K/k)$ are cyclic, then all decomposition groups in N_ν^n/k are cyclic. Now given any semidirect product $P \rtimes G$, with P a finite p-group, there exist some n, ν and an operator epimorphism from $\mathcal{F}(n)/\mathcal{F}(n)^{(\nu)}$ to P, and a corresponding epimorphism from the semidirect product $\mathcal{F}(n)/\mathcal{F}(n)^{(\nu)} \rtimes G$ to $P \rtimes G$. This implies that the split embedding problem associated with the epimorphism $P \rtimes G \twoheadrightarrow G$ has a proper solution with solution field $N \subseteq N_\nu^n$, and if all decomposition groups in $G(K/k)$ are cyclic, then all decomposition groups in $G(N/k)$ are cyclic. Finally, given any semidirect product $Q \rtimes G$ with Q a finite nilpotent group, the above argument implies that the embedding problem associated with the epimorphism $Q \rtimes G \twoheadrightarrow G$ has a proper solution with solution field M, and if all decomposition groups in $G(K/k)$ are cyclic, then all decomposition groups in M/k are cyclic.

Now the proof of Shafarevich's theorem follows by applying a theorem of Ore: let G be a finite solvable group. Then G has a nilpotent normal subgroup Q and a proper subgroup H such that $G = QH$. By induction we may assume H is realized as a Galois group $G(K/k)$ with all decomposition groups cyclic. Consider the semidirect product $Q \rtimes H$ with H acting on Q by conjugation inside G. By the above, the embedding problem associated with the epimorphism $Q \rtimes H \twoheadrightarrow H$ has a proper solution with solution field M, and since all decomposition groups in $G(K/k)$ are cyclic, all decomposition groups in M/k are cyclic. Finally, since G is a homomorphic image of $Q \rtimes H$, there is a subfield L of M such that L/k is Galois with group G and all decomposition groups cyclic. This verifies the observation about Shafarevich's construction and completes the proof of the theorem. $\square$

Remark. Proposition 1 and Theorem 2 hold with the base field $\mathbb{Q}$ replaced by an arbitrary global field k, with the same proof, where the primes p are replaced by the primes of k.

We now turn to nonsolvable groups. One family of groups each of which is the union of two conjugacy classes of proper subgroups is the family of Frobenius groups. Unlike most nonsolvable groups, nonsolvable Frobenius groups are known to be realizable as Galois groups over $\mathbb{Q}$ [So]. If G is a Frobenius group, then G is a semidirect product $Q \rtimes H$, where $g^{-1}Hg \cap H = 1$ for all $g \notin H$, which implies that G is covered by Q (which is normal) and the conjugates of H [Hu, p. 495].

Theorem 3. *Let G be a Frobenius group. Then there exists a polynomial $f(x)$ which is the product of two irreducible polynomials in $\mathbb{Q}[x]$ with Galois group G and having a root in $\mathbb{Q}_p$ for all rational primes p.*

The proof of this theorem will use the following group-theoretic lemma, for which we are indebted to David Chillag.

Lemma 1. *Let G be a Frobenius group $Q \rtimes H$. Then every subgroup D of G such that $D \cap Q = \{1\}$ is contained in a conjugate of H.*

Proof. Since $D \cap Q = \{1\}$, every element of D acts without fixed points on Q, so DQ is a Frobenius group with kernel Q and complement D. By [Hu, Thm. 8.18, p. 506], the center of any Frobenius complement and in particular, $Z(D)$, is nontrivial. Let d be a nontrivial element of $Z(D)$. Then $D \subseteq C(d)$, where $C(d)$ is the centralizer of d in G. d lies in a conjugate of H, so without loss of generality, we may assume $d \in H$. On the other hand, $C(d) \subseteq H$, since if $x \in C(d) \setminus H$, then $xdx^{-1} = d$ lies in $xHx^{-1} \cap H = \{1\}$, contradiction. We therefore have $D \subseteq H$. $\square$

Proof of Theorem 2.3. By Proposition 1, it suffices to show that G is realizable as the Galois group of an extension $K/\mathbb{Q}$ with each decomposition group contained in either Q or a conjugate of H; hence by Lemma 1, it suffices to show that G is realizable as the Galois group of an extension $K/\mathbb{Q}$ such that each decomposition group is either contained in Q or intersects Q trivially. We now proceed to show this. One fact about Frobenius groups is very relevant here, namely Thompson's theorem that the Frobenius kernel Q of G is nilpotent [Hu, p. 499, Thm. 8.7] (in fact for G nonsolvable, Q is even abelian [Hu, p. 506, Thm. 8.18]). We may therefore use Shafarevich's theorem as we did in the proof of Theorem 2. The same argument that we used there shows that if we can realize the Frobenius complement H by a Galois extension $L/\mathbb{Q}$, then we can embed $L/\mathbb{Q}$ into a Galois extension $K/\mathbb{Q}$ with group G such that the ramified primes in $L/\mathbb{Q}$ split completely in K/L, and the ramified primes of K/L are split completely in $L/\mathbb{Q}$. Let $\mathfrak{p}$ be a prime of K. If it is unramified over $\mathbb{Q}$, its decomposition group is cyclic, hence contained in either Q or a conjugate of H. If it is ramified over $\mathbb{Q}$, let $I(\mathfrak{p})$ be its inertia group. If $I(\mathfrak{p}) \subseteq Q$, then $\mathfrak{p}$ is unramified in $L/\mathbb{Q}$ and ramified in K/L, hence split completely in $L/\mathbb{Q}$, so its decomposition group is contained in Q (and in fact equals $I(\mathfrak{p})$) and we are done. Otherwise, $I(\mathfrak{p})$ is not contained in Q, so $\mathfrak{p}$ is ramified in $L/\mathbb{Q}$, and so splits completely in K/L. This means that its decomposition group $G(\mathfrak{p})$ intersects Q trivially.

The proof of Theorem 3 is then completed by the realization of nonsolvable Frobenius complements over $\mathbb{Q}$ in [So]. □

Remark 1. Theorem 3 holds with $\mathbb{Q}$ replaced by an arbitrary number field k.

Proof. It suffices to realize every nonsolvable Frobenius complement H as the Galois group of a geometric (regular over $\mathbb{Q}$) extension of the rational function field $\mathbb{Q}(t)$, since Hilbert's Irreducibility Theorem implies that if a group G is realizable as the Galois group of a geometric extension of $\mathbb{Q}(t)$, then it is realizable over every number field. Now H is itself a semidirect product $Z \rtimes B$, where Z is the semidirect product of two cyclic groups of orders relatively prime to each other and to $2, 3, 5$, and B is one of two groups: $\hat{A}_5$, the double cover of the alternating group A_5, or $\hat{S}_5$, one of the two double covers of the symmetric group S_5. Over any Hilbertian field F, every split geometric embedding problem with abelian kernel has a proper geometric solution [MM, Thm. 2.4, p. 275]. Two applications of this fact reduce the proof to the geometric realization of $\hat{A}_5$ and $\hat{S}_5$ over $\mathbb{Q}(t)$, which appear in [Me] and [Soa], respectively. □

The proof of Remark 1 implies a result that does not seem to have been observed before:

Theorem 4. *Every nonsolvable Frobenius group is realizable as the Galois group of a geometric extension of* $\mathbb{Q}(t)$.

Proof. As mentioned earlier, the Frobenius kernel of a nonsolvable Frobenius group is abelian. Since the Frobenius complement is realizable geometrically over $\mathbb{Q}(t)$, another application of [MM, Thm. 2.4, p. 275] yields the result. □

Remarkably, this result is not known for solvable Frobenius groups in general, since nonabelian Frobenius kernels are known to exist.

Note added in proof. A finite nonsolvable group G is realizable as the Galois group over $\mathbb{Q}$ of a polynomial $f(x) \in \mathbb{Q}[x]$ having no rational roots and having a root in $\mathbb{Q}_p$ for all rational primes p if and only if G is realizable as a Galois group over $\mathbb{Q}$.

References

[BeBi] D. Berend and Y. Bilu, *Polynomials with roots modulo every integer*, Proc. AMS **124** (1996), 1663-1671. MR1307495 (96h:11107)

[Br] R. Brandl, *Integer polynomials with roots mod p for all primes p*, J. Alg. **240** (2001), 822-835. MR1841358 (2002e:12003)

[BBH] R. Brandl, D. Bubboloni and I. Hupp, *Polynomials with roots mod p for all primes p*, J. Group Th. **4** (2001), 233-239. MR1812329 (2002f:12002)

[Hu] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967. MR0224703 (37:302)

[Me] J.-F. Mestre, *Extensions régulières de Q(T) de groupe de Galois* $\tilde{A}_n$, J. Algebra **131** (1990), 483-495. MR1058560 (91j:12010)

[MM] G. Malle and B. Matzat, *Inverse Galois Theory*, Springer-Verlag, Berlin, 1999. MR1711577 (2000k:12004)

[NSW] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, Springer-Verlag, Berlin, 2000. MR1737196 (2000j:11168)

[So] J. Sonn, *SL(2,5) and Frobenius Galois groups over* $\mathbb{Q}$, Canad. J. Math **32** (1980), 281-293. MR571923 (81g:12009)

[Soa] J. Sonn, *Central extensions of* S_n *as Galois groups of regular extensions of* $\mathbb{Q}(T)$, J. Alg. **140** (1991), 355-359. MR1120428 (92g:12007)

Department of Mathematics, Technion, 32000 Haifa, Israel
E-mail address: sonn@math.technion.ac.il