

IRREDUCIBLE POLYNOMIALS WHICH ARE LOCALLY REDUCIBLE EVERYWHERE

ROBERT GURALNICK, MURRAY M. SCHACHER, AND JACK SONN

(Communicated by Martin Lorenz)

ABSTRACT. For any positive integer n , there exist polynomials $f(x) \in \mathbb{Z}[x]$ of degree n which are irreducible over \mathbb{Q} and reducible over \mathbb{Q}_p for all primes p if and only if n is composite. In fact, this result holds over arbitrary global fields.

1. INTRODUCTION

Hilbert gave examples of irreducible polynomials $f(x) \in \mathbb{Z}[x]$ of degree 4 which are reducible mod p for all primes p , namely $x^4 + 2ax^2 + b^2$. Note that this polynomial is irreducible over $\mathbb{Q}(a, b)$, hence (by Hilbert's irreducibility theorem) is irreducible over \mathbb{Q} for infinitely many specializations of a and b into \mathbb{Q} . The underlying reason for this phenomenon from the Galois-theoretic point of view is that the Galois group of $x^4 + 2ax^2 + b^2$ over $\mathbb{Q}(a, b)$ is Klein's four group. Therefore for any p not dividing the discriminant of f , the decomposition group is a cyclic group of order at most 2, so f is reducible mod p . (Note that for p dividing the discriminant of f , f is reducible mod p as well.) The phenomenon is thus forced by the structure of the Galois group. This also explains why there can be no such examples of polynomials of prime degree. Indeed, suppose $f(x) \in \mathbb{Z}[x]$ has prime degree ℓ and is irreducible in $\mathbb{Z}[x]$. Then its Galois group has an element of order ℓ , so by Chebotarev's density theorem there exists p such that the splitting field of f over \mathbb{F}_p has Galois group C_ℓ , the cyclic group of order ℓ ; hence f must be irreducible over \mathbb{F}_p . We will give a proof that the degree of f being prime is the only obstacle, namely that for any composite n , there exist irreducible $f(x) \in \mathbb{Z}[x]$ of degree n which are reducible mod p for all p . Brandl [2] has proved the same result by similar methods. We give a short proof of a generalization of this.

In fact, there is an irreducible $f(t, x) \in \mathbb{Z}[t, x]$ of degree n such that $f(t_0, x)$ is reducible mod p for all specializations $t = t_0$ in \mathbb{Z} and all p . We will also prove the more delicate result that for any composite n , there exist irreducible $f(x) \in \mathbb{Q}[x]$ of degree n which are reducible over \mathbb{Q}_p for all p , and that this result generalizes to arbitrary global fields. Note that Hilbert's example does not satisfy this last condition for all a, b , e.g. $x^4 + 1$ is irreducible over \mathbb{Q}_2 .

Received by the editors April 3, 2004 and, in revised form, June 17, 2004.

2000 *Mathematics Subject Classification*. Primary 11R52, 11S25, 12F05, 12G05, 16K50.

The first author was partially supported by NSF Grant DMS 0140578. The research of the third author was supported by Technion V.P.R. Fund-S. and N. Grand Research Fund.

It is worthwhile pointing out here that a random polynomial $f(x) \in \mathbb{Z}$ of composite degree n is not reducible mod p for all p , as its Galois group over \mathbb{Q} is S_n [6], and since S_n contains an n -cycle, Chebotarev's density theorem implies that there are infinitely many primes p for which $f(x)$ is irreducible mod p .

2. MOD p REDUCIBILITY

Let $f(x) \in \mathbb{Z}[x]$ be monic irreducible of degree n with Galois group G over \mathbb{Q} . As in the discussion above, we see that if $f(x)$ is irreducible mod p , then p does not divide the discriminant of $f(x)$, and G must contain an element of order n , since the decomposition group is cyclic of order n . Thus if G has no element of order n , then f must be reducible mod p for all p . On the other hand, since f is irreducible over \mathbb{Z} , G has a subgroup H of index n . More generally, if K/\mathbb{Q} is a finite Galois extension with Galois group G , and if G has a subgroup H of index n but no element of order n , then the fixed field, say $\mathbb{Q}(\theta)$, of H has degree n and the minimal polynomial f of θ over \mathbb{Q} has degree n with splitting field $L \subseteq K$, Galois group $\bar{G} = G(L/\mathbb{Q}) \cong G/\text{core}(H)$ where $\text{core}(H)$ is the intersection of the conjugates of H . Furthermore, \bar{G} has a subgroup \bar{H} of index n but has no element of order n , so f is reducible mod p for every p . In summary:

Lemma 2.1. *Let G be a finite group and n a positive integer such that*

- 1) G is realizable as a Galois group $G(K/\mathbb{Q})$,
- 2) G has a subgroup of index n , but G has no element of order n .

Then there is an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n which is reducible mod p for all primes p (with splitting field contained in K).

In connection with Hilbert's example, it follows from the preceding considerations that a polynomial of degree four has the property of being irreducible over \mathbb{Z} and reducible mod p for all p if and only if its Galois group over \mathbb{Q} is either Klein's four group V_4 or the alternating group A_4 .

Theorem 2.2. *For any composite positive integer n , there exist irreducible polynomials $f(x) \in \mathbb{Z}[x]$ of degree n which are reducible mod p for all primes p .*

Proof. By the lemma, it suffices to find G satisfying conditions 1) and 2).

Case 1. n squarefree. Write $n = qm$ with q prime, so $(m, q) = 1$. Let t be the order of q mod m and set $G = C_m \rtimes V$ (semidirect product), where V denotes the additive group of \mathbb{F}_{q^t} with C_m acting by multiplication by the m th roots of unity $\mu_m \subset \mathbb{F}_{q^t}$, where we identify C_m with μ_m . The action of C_m on V is faithful and 0 is the only fixed point. Let H be a hyperplane in V , i.e. $[V : H] = q$. Then $[G : H] = qm = n$. Furthermore, if $g \in G$ had order n , then $g^m (\in V)$ would have order q and be fixed by g , hence by C_m , a contradiction.

We therefore have found for every squarefree composite n , a solvable group G satisfying condition 2). By Shafarevich's theorem (in fact by an older theorem of Scholz), G is realizable as a Galois group over \mathbb{Q} .

Case 2. n not squarefree. Assume first that $n = q^2$, q prime. Then $G_1 := C_q \times C_q$ satisfies 2) with H the trivial group. For arbitrary $n = q^2m$, take $G := G_1 \times C_m$ which again has the trivial subgroup of index n and no element of order n . \square

We now remark that since the groups G appearing in the proof can be realized regularly over the rational function field $\mathbb{Q}(t)$ (see e.g. [4, p. 275]), we obtain irreducible polynomials $f(t, x) \in \mathbb{Z}[t, x]$ of degree n which by Hilbert's irreducibility

theorem have infinitely many specializations of t into \mathbb{Q} which are irreducible with Galois group G , hence reducible mod p for all p .

3. p -ADIC REDUCIBILITY

We now wish to prove Theorem 2.2 with reducibility mod p replaced by reducibility over \mathbb{Q}_p . The preceding construction actually yields irreducible polynomials $f(x) \in \mathbb{Z}[x]$ which are reducible over \mathbb{Q}_p for all primes which are unramified in the splitting field of f , but may be irreducible over \mathbb{Q}_p for ramified p . The proof will be similar but more delicate.

Let $f(x) \in \mathbb{Q}[x]$ be irreducible and let p be a prime. Let K be the splitting field of f over \mathbb{Q} , $G = G(K/\mathbb{Q})$, \mathfrak{p} a prime of K over p , $D = D(\mathfrak{p})$ the decomposition group. Then f is irreducible over \mathbb{Q}_p if and only if $D(\mathfrak{p})$ acts transitively on the roots of f in K . Let H be the subgroup of G fixing a root of f . The action of G on the roots of f is equivalent to its action by multiplication from the left on the left cosets of H in G . Thus f is irreducible over \mathbb{Q}_p if and only if $D(\mathfrak{p})$ acts transitively on the left cosets of H in G , i.e. the set product DH is equal to G . Suppose K/\mathbb{Q} were tamely ramified, so that all the decomposition groups were metacyclic. Then in order to insure that f is reducible over all \mathbb{Q}_p , it would suffice that (the set product) $MH \neq G$ for every metacyclic subgroup M of G . We therefore have the following lemma.

Lemma 3.1. *Let G be a finite group and n a positive integer such that*

3) *G is realizable over \mathbb{Q} by a tamely ramified extension K/\mathbb{Q} ,*

4) *G has a subgroup H of index n , the intersection of whose conjugates is trivial, such that the set product $MH \neq G$ for every metacyclic subgroup M of G .*

Then there exists an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree n (with splitting field K) which is reducible over \mathbb{Q}_p for all primes p .

Theorem 3.2. *For any composite positive integer n , there exist irreducible polynomials $f(x) \in \mathbb{Q}[x]$ of degree n which are reducible over \mathbb{Q}_p for all primes p .*

Proof. By Lemma 3.1, it suffices to find G satisfying 3) and 4).

Case 1. n squarefree. The same G and H work as in the proof of Theorem 2.2, provided the order t of $q \bmod m$ is greater than 1 (which can be ensured by taking q to be the smallest prime dividing n). Indeed, V has \mathbb{F}_q -dimension t and is irreducible as a C_m -module, so in this case the only metacyclic subgroups of G are cyclic of order q or a divisor of m . Thus condition 4) is satisfied.

Condition 3) can be proved using Saltman's results, [5, Theorem 3.5] to verify that G has a generic Galois extension and then [5, Theorem 5.9] to see that there exists a tame extension realizing G .

Case 2. n not squarefree. As in the proof of Theorem 2.2, we first assume $n = q^2$, q a prime. We will construct a Galois extension K/\mathbb{Q} with Galois group $C_q \times C_q$, with local degree 1 or q at all primes p . If $K = \mathbb{Q}(\theta)$ with $f(x)$ the minimal polynomial of θ over \mathbb{Q} , then f has the desired property. As we saw earlier, for any prime unramified in K the decomposition group is cyclic, so the local degree is 1 or q just from the structure of G . We need to construct K so that the local degree is q at the ramified primes. For this we use an idea from [3].

Let ℓ be a prime congruent to 1 mod q and let $L_\ell \subseteq \mathbb{Q}(\mu_\ell)$ such that $G(L_\ell/\mathbb{Q}) \cong C_q$. We seek another prime r such that

5) $r \equiv 1 \pmod{q}$,

- 6) r splits completely in L_ℓ ,
- 7) ℓ splits completely in L_r .

If r satisfies these conditions, then clearly $K = L_\ell L_r$ will have the local degree at most q everywhere.

5) is equivalent to the condition that r splits completely in $\mathbb{Q}(\mu_q)$. 7) is equivalent to the condition that the Frobenius automorphism of ℓ in $G(\mathbb{Q}(\mu_r)/\mathbb{Q})$ fixes L_r pointwise, i.e. is a q th power in the cyclic group $G(\mathbb{Q}(\mu_r)/\mathbb{Q})$, which is equivalent to ℓ being a q th power mod r , which in turn means that the polynomial $x^q - \ell$ has a root mod r . Since \mathbb{F}_r contains the q th roots of unity, this is equivalent to $x^q - \ell$ factoring into linear factors mod r , which is equivalent to the condition that r splits completely in $\mathbb{Q}(\mu_q, \sqrt[q]{\ell})$. It follows that conditions 5), 6), 7) together are equivalent to the condition that r splits completely in $L_\ell(\mu_q, \sqrt[q]{\ell})$. By Chebotarev's density theorem, such an r exists. This completes the case $n = q^2$.

Now assume the general case $n = q^2 m$, q prime. Let K be as in the case $n = q^2$, and let L be any abelian extension of \mathbb{Q} of degree m such that $K \cap L = \mathbb{Q}$. (For example, choose a prime $p \equiv 1 \pmod{m}$, $p \neq \ell, r$, and let $L \subseteq \mathbb{Q}(\mu_p)$ of degree m over \mathbb{Q} .) KL/\mathbb{Q} has degree n , and the local degree at any prime is at most $qm < n$. \square

4. GLOBAL FIELDS

Theorem 3.2 generalizes to arbitrary global fields F . If n is prime and $f(x) \in F[x]$ is a separable monic irreducible polynomial, then by Chebotarev's density theorem, which holds over any global field [7, p. 289], there exist primes \mathfrak{p} of F such that f is irreducible over the completion $F_{\mathfrak{p}}$. (Even if n is equal to the characteristic p of F , and $f(x)$ is inseparable of degree p , i.e. $f(x) = x^p - a$, then by [1, Chapter 9, Theorem 1], if $f(x)$ is irreducible, then $f(x)$ is irreducible over $F_{\mathfrak{p}}$ for infinitely many \mathfrak{p} .)

Theorem 4.1. *For any composite positive integer n , and any global field F , there exist irreducible polynomials $f(x) \in F[x]$ of degree n which are reducible over $F_{\mathfrak{p}}$ for all primes \mathfrak{p} of F .*

Proof. If F is a number field, one can reduce the proof to the case $F = \mathbb{Q}$. Let $f(x) \in \mathbb{Q}[x]$ be irreducible of degree n and reducible over \mathbb{Q}_p for all p , and suppose its splitting field K satisfies $K \cap \mathbb{Q} = \mathbb{Q}$. Then $f(x)$ is irreducible over F and is reducible over $F_{\mathfrak{p}}$ for all primes \mathfrak{p} of F . It remains to observe that the proof of Theorem 3.2 produces infinitely many \mathbb{Q} -linearly disjoint extensions K with the desired properties. We may therefore assume that F a global function field of characteristic p .

Let $f(x) \in F[x]$ be monic irreducible of degree n , fix a root α in a splitting field K , let $G = G(K/F)$, and let $H = G(K/F(\alpha))$. Let \mathfrak{p} be a prime of F , \mathfrak{P} a prime of K dividing \mathfrak{p} , $D = D(\mathfrak{P})$ the decomposition group. Then $f(x)$ is reducible over $F_{\mathfrak{p}}$ if and only if D does not act transitively on the roots of $f(x)$, i.e. the set DH is not equal to G . We reduce the proof to the case when n is a product of two primes, not necessarily distinct.

For any positive integer m , let E/F be a Galois (e.g. cyclic) extension of degree m such that $K \cap E = F$, with K as above. Assume for all primes \mathfrak{P} of K that $D(\mathfrak{P})H \neq G$. Let $\hat{K} = KE$, $\hat{G} = G(KE/F) \cong G \times G(E/F)$. Identify H with $H \times \{1\} \subset \hat{G}$. Then for any prime $\hat{\mathfrak{P}}$ of \hat{K} , $D(\hat{\mathfrak{P}})H \neq \hat{G}$. This reduces the proof

of Theorem 4.1 to the case when n is a product of two primes, say r and s . We will further reduce the proof to the case that F is a rational function field $\mathbb{F}_q(t)$, by constructing the desired $K/\mathbb{F}_q(t)$ linearly disjoint over $\mathbb{F}_q(t)$ from any F given in advance. Accordingly we now assume $F = \mathbb{F}_q(t)$. As we will see, when n is prime to p , one can give a proof which is analogous to that of Theorem 3.2.

Case 1. $r = s \neq p$. We use a function field analogue of a construction in [3]. Let $\mathfrak{p} = (h(t))$ be a (finite) prime of F ($h(t) \in \mathbb{F}_q[t]$) which splits completely in the extension F' of F obtained by adjoining all r th roots of all elements of \mathbb{F}_q (including the r th roots of unity). Then $Cl_F(\mathfrak{p})$, the ray class group mod \mathfrak{p} , is cyclic (the class group of F is trivial), and has order divisible by r . There is a corresponding ray class field extension $R^{\mathfrak{p}}/F$ which is geometric (regular over \mathbb{F}_q), $G(R^{\mathfrak{p}}/F) \cong Cl_F(\mathfrak{p})$, and \mathfrak{p} is the only prime that ramifies in $R^{\mathfrak{p}}$. Let $L^{\mathfrak{p}}$ be the (unique, cyclic) subfield of $R^{\mathfrak{p}}$ of degree r over F . We seek $\mathfrak{p}, \mathfrak{q}$ such that $K := L^{\mathfrak{p}}L^{\mathfrak{q}}$ has the desired property, which is that \mathfrak{p} splits completely in $L^{\mathfrak{q}}$ and \mathfrak{q} splits completely in $L^{\mathfrak{p}}$. Let \mathfrak{p} be as above, which exists e.g. by Chebotarev's density theorem (we don't really need Chebotarev yet since the extension is a constant extension, but presently we will need it). We seek \mathfrak{q} which satisfies the same conditions as does \mathfrak{p} , and additionally, \mathfrak{p} splits completely in $L^{\mathfrak{q}}$ and \mathfrak{q} splits completely in $L^{\mathfrak{p}}$. The last condition is an additional Chebotarev condition on \mathfrak{q} which is compatible with the preceding ones, so can be satisfied by Chebotarev's density theorem. The condition \mathfrak{p} splits completely in $L^{\mathfrak{q}}$ is equivalent to the condition that the Frobenius $Frob(\mathfrak{p})$ is an r th power in $G(R^{\mathfrak{q}}/F)$, which is equivalent to $\mathfrak{p} = h(t)$ being an r th power in $Cl_F(\mathfrak{q})$, which is equivalent to $h(t)$ being an r th power in the multiplicative group of the residue field $\mathbb{F}_q[t]/\mathfrak{q}$, which is equivalent to \mathfrak{q} splitting completely in $F(\sqrt[r]{h(t)})$. This is another Chebotarev condition on \mathfrak{q} compatible with the preceding ones. The construction yields infinitely many linearly disjoint extensions K , completing the proof of this case.

Case 2. $r \neq s$, both $\neq p$. Here we can argue exactly as in the case n squarefree in the proof of Theorem 3.2, by constructing a tamely ramified G -extension using Saltman's results as quoted earlier. This yields infinitely many linearly disjoint extensions.

Case 3. $r = s = p$. We seek a pair of Artin-Schreier extensions L, M defined by $x^p - x - g(t), x^p - x - h(t)$ respectively, where $g(t), h(t) \in F$, such that $K := LM$ has local degree 1 or p everywhere. Let $g(t)$ be a polynomial without constant term, i.e. $g(0) = 0$. Since the derivative of $x^p - x - g(t)$ with respect to x is -1 , the only prime of F that ramifies in L is infinity. Furthermore, the prime corresponding to t splits completely in L since $x^p - x - g(t)$ has p distinct roots mod t . The automorphism $t \mapsto 1/t$ interchanges (t) and infinity. Let $h(t) = g(1/t)$. Then infinity splits completely in M and (t) is the only ramified prime in M . It follows that the local degree of LM is 1 or p everywhere, as desired. We get infinitely many linearly disjoint extensions by varying $g(t)$, e.g. by taking $g(t)$ of the form t^e , with e prime to p . The genus of the corresponding curve grows with e , or one can show that there are infinitely many such distinct extensions even over the completion of F at infinity.

Case 4. $r = p \neq s$.

Subcase 4.1. $p \nmid s - 1$. We can use the group G we used earlier. Let C_p act on an irreducible \mathbb{F}_s -space V , so $\dim(V) > 1$. Claim that $G := C_p \ltimes V$ cannot be a local Galois group anywhere. Indeed, if it were, the extension would be ramified,

so the inertia group would be a nontrivial normal subgroup of G , hence equal to V or G . There is no wild ramification, since G has no normal p -subgroup. But then the inertia subgroup must be cyclic, contradicting the fact that G has no cyclic normal subgroup. This proves the claim. It follows that all decomposition groups are proper subgroups of G . But if D is a proper subgroup of G , then DH cannot equal G , as is easily verified (see beginning of the previous section). It remains to show that G is realizable (infinitely often, linearly disjointly) over F . Realize C_p by an Artin-Schreier extension L/F (there are infinitely many), and consider the embedding problem with kernel V . It has a proper solution since F is Hilbertian [4, p. 275].

Subcase 4.2. $p|s-1$. Here the roles of p and s need to be interchanged, and we have to worry about wild ramification. (The argument will also cover subcase 4.1.) Let E/F be a cyclic regular extension of degree s . Claim there exists an Artin-Schreier extension L/E of degree p such that every prime \mathfrak{q} of E that ramifies in L is split completely over F and all its remaining $s-1$ conjugates over F are unramified in L . Indeed, there are infinitely many primes \mathfrak{p} of F that split completely in E . Let $\{\mathfrak{p}_i\}$ be a sequence of such primes and let \mathfrak{q}_i be a prime of E dividing \mathfrak{p}_i for each i . Let $h = h_E$ be the class number of E . Then in the sequence $\mathfrak{q}_1, \mathfrak{q}_1\mathfrak{q}_2, \dots, \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_{h+1}$ of ideals of E , there must be two which differ by a principal ideal (f) ; i.e., there exist $i \leq j \in \{1, 2, \dots, h+1\}$ such that $\mathfrak{q}_i \cdots \mathfrak{q}_j = (f)$ with $f \in E^*$. Take L/E to be the Artin-Schreier extension defined by the equation $x^p - x = 1/f$. Since the only poles of $1/f$ are $\mathfrak{q}_i, \dots, \mathfrak{q}_j$, the only ramified primes in L/E are also $\mathfrak{q}_i, \dots, \mathfrak{q}_j$. Furthermore, since these are simple poles, the extension L/E is nontrivial (of degree p). This proves the claim. Let M/F be the Galois closure of L/F , and set $W = G(M/E)$. By construction, the conjugates of L over F are linearly disjoint over E , so W is isomorphic to the group ring $\mathbb{F}_p C_s$ as C_s -modules, identifying $G(E/F)$ with C_s . There is an irreducible submodule V of W on which C_s acts faithfully. The \mathbb{F}_p -dimension of V is necessarily greater than 1 since $s > p$. Let K be the subfield of M corresponding to the complementary submodule to V in W (by Maschke's theorem). Then K/F is Galois with group $G = C_s \times V$. Let H be a subgroup of V of index p . We show that H has the desired property, that $DH \neq G$ for any decomposition group D . The argument is similar to previous ones. If D is the decomposition group of an unramified prime, then D is cyclic. Since G has no cyclic subgroup of order sp , D has order p or s ; hence DH cannot equal G . At a tamely ramified prime, the inertia group must be of order s and be normal in D . So D is either cyclic of order s , and $DH \neq G$, or D is of order sp with a normal p -Sylow subgroup, which cannot happen because D has no element of order sp . Finally, the decomposition group of a wildly ramified prime in K/F must be contained in V , since such a prime must divide one of $\mathfrak{q}_i, \dots, \mathfrak{q}_j$, and C_s does not fix any of them. Hence again $DH \neq G$. Finally, there are infinitely many linearly disjoint extensions E/F , hence infinitely many linearly disjoint extensions K/F . The proof is complete. \square

REFERENCES

- [1] E. Artin and J. Tate, *Class Field Theory*, Harvard University, Cambridge, 1961. MR1043169 (91b:11129)
- [2] R. Brandl, *Integer polynomials that are reducible modulo all primes*, Amer. Math. Monthly **93** (1986), 286-288. MR0835298 (87f:12007)

- [3] H. Kisilevsky and J. Sonn, *On the n -torsion subgroup of the Brauer group of a number field*, J. Th. Nombres de Bordeaux **15** (2003), 199-204. MR2019011 (2004j:11142)
- [4] G. Malle and B.H. Matzat, *Inverse Galois Theory*, Springer-Verlag, Berlin, 1999. MR1711577 (2000k:12004)
- [5] David Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), 250-283. MR0648801 (84a:13007)
- [6] B. L. Van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann. **109** (1934), 13-16.
- [7] A. Weil, *Basic Number Theory, third ed.*, Springer-Verlag, Berlin, 1974. MR0427267 (55:302)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CALIFORNIA 90089-2532

E-mail address: `guralnic@usc.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA AT LOS ANGELES, LOS ANGELES, CALIFORNIA 90024

E-mail address: `mms@math.ucla.edu`

DEPARTMENT OF MATHEMATICS, TECHNION, 32000 HAIFA, ISRAEL

E-mail address: `sonn@math.technion.ac.il`