LOCAL-GLOBAL PRINCIPLE FOR n^{th} POWERS

ISHAN LEVY

Given a number field F, when is $a \in F$ an n^{th} power modulo every prime? Here the question will be answered for many F including $\mathbb{Q}$ (and the technique in principle probably works for any F with some calculation).

Theorem 0.1. *Suppose F is a field. If $4|n$, then $x^n - a$ is reducible iff if a is a p^{th} power for some $p|n$ or if a is of the form $-4k^4$ and $\operatorname{char} F \neq 2$. If $4 \nmid n$, then $x^n - a$ is irreducible iff a is not a p^{th} power mod every $p|n$.*

Proof. First reduce to the case of a prime power. Suppose $x^n - a, x^m - a$ are irreducible and $(n, m) = 1$. Then $F[a^{\frac{1}{m}}]$ is degree n and $F[a^{\frac{1}{n}}]$ is degree m, so their compositum, $F[a^{\frac{1}{m}n}]$ is degree mn, so $x^{nm} - a$ is irreducible. Conversely, if either is reducible, $x^{nm} - a$ is reducible.

The prime power case will be done by induction on the power. If $x^{p^m - a}$ is irreducible, then $x^{p^{m+1}} - a$ is reducible iff $a^{\frac{1}{p^m}}$ is a p^{th} power in $F[a^{\frac{1}{p^m}}]$. But if this is true, then its norm down to F is also a p^{th} power. The norm is a unless $p = 2$, in which case it is $-a$. Thus a, or $-a$ is a p^{th} power, a contradiction if $p > 2$ or $m > 1$. If $p = 2, m = 1, \operatorname{char} F \neq 2$, then $F[\sqrt{a}] = F[i]$. Now calculation shows ki is a square iff k is of the form $(1+i)^2y^2$, some $y \in F$, so a is of the form $-4y^4$. In this case, conversely $(-4y^4)^{1/4} = (1+i)y$ is degree 2 over F, so the polynomial $x^4 + 4y^4$ is reducible. If $\operatorname{char} F = 2$, then $-a = a$, so a is a square, a contradiction.

In the case n is a prime p, If $x^p - a$ factors with some polynomial $f = x^i + \dots$, where $i < p$, then the norm of a root α of f from $F[\alpha]$ to F will be $\alpha^{i/p}$, which is an integer iff α^i is a p^{th} power iff α is a p^{th} power. □

Let F be a number field.

Lemma 0.2. *Let $a \in F$ be an n^{th} power modulo every prime. Then $a^{\frac{1}{n}} \in F[\zeta_n]$.*

Proof. Let K be the splitting field of $x^n - a$. If a prime splits in K, it splits completely in the subfield $F[\zeta_n]$. Conversely, if it splits completely in $F[\zeta_n]$, the polynomial $x^n - a$ has a root mod p so it factors into linear factors as ζ_n is there. Thus if the prime doesn't divide the discriminant, then it splits completely in K. Up to a finite set, the same primes split in $F[\zeta_n]$ and K so $K = F$. □

Corollary 0.3. *Let q be prime. If $a \in F$ is a q^{th} power mod every prime, it is a q^{th} power.*

Proof. $a^{1/q} \in F[\zeta_q]$, but $[F[\zeta_q] : F] = q - 1$ is relatively prime to q so $a \in F$. □

Now suppose that the cyclotomic polynomials are irreducible over F, i.e. for all n, $F \cap \mathbb{Q}[\zeta_n] = \mathbb{Q}$.

Lemma 0.4. *Let q be either a prime or 4 and suppose $x^q - a$ is irreducible over F and if $q = 4$ suppose $-a$ is not a square in F. Then the Galois group of $x^q - a$ is $\operatorname{Hol}(\mathbb{Z}/q\mathbb{Z}) = \mathbb{Z}/q\mathbb{Z} \rtimes \operatorname{Aut}(\mathbb{Z}/q\mathbb{Z})$.*

Proof. This problem amounts to showing that $F[a^{\frac{1}{q}}]$ is linearly disjoint over F from $F[\zeta_q]$. Indeed, if that is true, then the degree of the splitting field will be the degree of the compositum which is $\phi(q)q$. There are $\phi(q)$ conjugates of ζ_q and q conjugates of $a^{\frac{1}{q}}$, so the Galois group must act transitively on the pairs of conjugates of ζ_q and $a^{\frac{1}{q}}$, giving an isomorphism with $\mathrm{Hol}(\mathbb{Z}/q\mathbb{Z})$. In the case that q is prime, linearly disjointness follows from the degrees being relatively prime. In the case that $q = 4$, one simply has to note that since $a, -a$ are not squares, $x^4 - a$ is irreducible in $F[i]$. □

Corollary 0.5. *For a not a q^{th} power for q an odd prime, $a^{1/q}$ doesn't lie in any cyclotomic extension of F. If $\pm a$ is not a square, then $a^{\frac{1}{4}}$ doesn't lie in a cyclotomic extension.*

Proof. If it did, then the Galois group of $x^q - a$ would be abelian by above, but it is not. □

Theorem 0.6. *For an odd prime power q^n, if a is a $(q^n)^{th}$ power mod every prime then a is a $(q^n)^{th}$ power.*

Proof. Suppose the theorem holds for $n - 1$. Then $a = b^{q^{n-1}}$ by hypothesis, and $a^{\frac{1}{q^n}} = b^{\frac{1}{q}} \in F[\zeta_{q^n}]$, so by applying the previous corollary to b, b is a q^{th} power in F. □

Theorem 0.7. *If a is a $(2^n)^{th}$ power mod every prime, either a is a $(2^n)^{th}$ power or $n \geq 3$ and a is $2^{2^{n-1}}$ times a $(2^n)^{th}$ power.*

Proof. For $n = 2$, $a = b^2$, and $\sqrt{b} \in F[i] \implies b = \pm k^2$ for some $k \in F$. Then $k^4 = a$. For $n \geq 3$ assume the theorem holds for $n-1$, $a = b^{2^{n-1}}$ or $2^{2^{n-2}} b^{2^{n-1}}$, and $\sqrt{b}$ or $(2b^2)^{\frac{1}{4}} \in F[\zeta_{2^n}]$. If $\sqrt{b} \in F[\zeta_{2^n}]$, $\sqrt{b}$ lies in a quadratic subfield of $F[\zeta_{2^n}]$ which must be in $F[\zeta_8]$ so $b = \pm k^2$ or $b = \pm 2k^2$, and $a = k^{2^n}, 2^{2^{n-1}} k^{2^n}$. If $(2b^2)^{\frac{1}{4}} \in F[\zeta_{2^n}]$, note that by the corollary, $\pm 2b^2 = c^2$, which is impossible. Thus $a = 2^{2^{n-1}} c^{2^n}$. □

Finally here is another problem of this sort:

Theorem 0.8. *Let f be an irreducible polynomial of degree n with coefficient in a number field F. Let G be the Galois group of K, the splitting field of f, and let $G \to S_n$ be the action of G on the roots of f. Then some element of G acts as an n-cycle iff f is irreducible modulo every prime.*

Proof. If f is not separable mod some p, then it can't be irreducible mod p. So we can ignore those primes. For the rest of the primes, note that how p splits in $F[\alpha]$, α a root of f, depends on the cycle structure of Frobenius. In particular, it is an n-cycle iff p is inert. But if G has some n-cycle, then by Chebotarev density theorem it is realized by some prime. Thus f is reducible mod all p iff p is never inert iff there is no n-cycle. □

The action of G on S_n is transitive, and is its action on G/H, where H is the subgroup of index n corresponding to the subfield generated by one root of f. Then some $g \in G$ acts as an n-cycle iff $\langle g \rangle H = G$. In particular, suppose that adjoining one root of f gives a Galois extension, so that H is trivial. Then G is not cyclic iff f is reducible modulo every prime. This lets us produce lots of examples, by choosing primitive elements of Galois extensions with non-cyclic Galois groups. For example, $x^4 + 1$ has ζ_8 a root, which has non-cyclic Galois group, and so $x^4 + 1$ is reducible modulo every prime.

Theorem 0.9. *Let f be a polynomial with $\mathcal{O}_K$ coefficients over a number field K. Let G be the Galois group of f, let a_i be the roots of f, and let G_i be the subgroup of G fixing $K[a_i]$. Then f has a root modulo (almost) every prime iff $\cup G_i = G$.*

Proof. By the Chebotarev density theorem, some prime has Frobenius not in $\cup G_i$ iff $\cup G_i \neq G$. An unramified prime $\mathfrak{p}$ lies in some G_i iff its Frobenius fixes some root a_i iff f has a root mod $\mathfrak{p}$. $\square$