

# Quasi-reducible Polynomials

Jacques Willekens

06-Dec-2008

## Abstract

In this article, we investigate polynomials that are irreducible over  $\mathbb{Q}$ , but are reducible modulo any prime number.

## 1 Introduction

Let  $f(x)$  be a polynomial with integer coefficients. As Gauss has shown, if  $f$  can be factored over  $\mathbb{Q}$ , it can also be factored over  $\mathbb{Z}$ ; in other words, the factors can be expressed using integer coefficients.

For a given prime  $p$ , let  $f_p(x)$  be the polynomial over  $\text{GF}(p)$  (the finite field of  $p$  elements) obtained by reducing the coefficients modulo  $p$ . If  $G$  is the Galois group of  $f$  over  $\mathbb{Q}$ , we will write  $G_p$  for the Galois group of  $f_p$  over  $\text{GF}(p)$ . As this defines a homomorphism from  $\mathbb{Z}[x]$  to  $\text{GF}(p)[x]$ , any factorization of  $f$  yields a corresponding factorization of  $f_p$ , obtained by reducing each factor separately. This shows that, if  $f$  is reducible (over  $\mathbb{Z}$ ), then  $f_p$  is also reducible (over  $\text{GF}(p)$ ) for any prime  $p$ . In many cases, this allows to prove that  $f$  is irreducible: if there is any prime  $p$  such that  $f_p$  is irreducible, then  $f$  is irreducible.

For example, this can be used to prove that a quadratic equation with odd integer coefficients has no rational root. Indeed, in this case, we have:

$$f_2(x) = x^2 + x + 1$$

and this polynomial is irreducible modulo 2; therefore, the original polynomial is irreducible, and, in the case of a second degree polynomial, this means that it has no rational root.

However, the converse of that proposition is not true: there are polynomials that are irreducible over  $\mathbb{Q}$ , but become reducible modulo any prime number. For the lack of a better word, we call these polynomials quasi-reducible. As we will show, there are infinitely many such polynomials; in fact, they are more frequent than one may expect.

## 2 General approach

We first recall some well-known results of Galois theory:

- If  $G$  is the Galois group of  $f$ ,  $G_p$  is the Galois group of  $f_p$ , then  $G_p$  is a subgroup of  $G$  (as an abstract group). The idea behind this is that  $f_p$  may be reducible, and any permutation of the roots must act separately on the roots of the irreducible factors of  $f_p$ .

Furthermore, if  $f_p$  has no repeated factors, there is a direct correspondence between the degrees of the irreducible factors of  $f_p$  and the cycle structure of an element of  $G$ , as a permutation group on the roots of  $f$ .

- Over any finite field  $\text{GF}(q)$ , the splitting field of a polynomial is  $\text{GF}(q^k)$  for some  $k$ , and the corresponding Galois group is cyclic and generated by the automorphisms  $x \mapsto x^q$ . The degree of the splitting field is the LCM of the degrees of the irreducible factors of the polynomial.

We will consider normal polynomials, i.e., minimal polynomials of a primitive element of a finite extension of  $\mathbb{Q}$ . Such a polynomial splits completely in the extension generated by a single root; therefore, the order of the Galois group is equal to the degree of the polynomial. We can find a monic integral normal polynomial for any finite extension, by choosing an algebraic integer as primitive element; we will only use such polynomials, to ensure that reduction modulo  $p$  preserves the degree of the polynomial.

Let  $f(x)$  be a normal (monic) polynomial of degree  $d$ . If the Galois group  $G$  is not cyclic,  $G$  cannot be the Galois group of a polynomial over  $\text{GF}(p)$ . Therefore,  $G_p$  is a proper subgroup of  $G$ , and has order less than  $d$ , which shows that  $f_p$  is reducible. As this holds for any prime  $p$ ,  $f$  is quasi-reducible.

If  $e$  is the exponent of the Galois group  $G$  of  $f(x)$ , and  $e_p$  the exponent of  $G_p$ , then  $e_p \leq e$ , as  $G_p$  is a subgroup of  $G$ . The degree of any irreducible factor of  $f_p$  divides  $e_p$ ; this means that, if we know  $e$ , this gives an upper bound on the degree of the irreducible factors of  $f_p$ .

### 3 Cyclotomic polynomials

Let us denote by  $\Phi_n(x)$  the cyclotomic polynomial of order  $n$ , i.e., the monic polynomial whose roots are the primitive  $n^{\text{th}}$  roots of unity. It is well known that  $\Phi_n(x)$  has rational integer coefficients and is irreducible over  $\mathbb{Q}$  (see [1, § 3.7]).  $\Phi_n(x)$  has degree  $\phi(n)$  (Euler's totient function), and its Galois group is  $U(n)$ , the multiplicative group of units of  $\mathbb{Z}_n$ .

$U(n)$  is the direct product of the groups  $U(p^k)$ , where the  $p^k$  are the prime powers occurring in the factorization of  $n$ . If  $p^k$  is such an odd factor,  $U(p^k)$  has even order, and therefore contains a subgroup isomorphic to  $C_2$ . Therefore, if  $n$  is divisible by two distinct odd primes,  $U(n)$  contains a subgroup isomorphic to  $C_2 \times C_2$ , and is not cyclic, which shows that  $\Phi_n(x)$  is quasi-reducible.

Furthermore, as  $U(4) \cong C_2$  and  $U(8) \cong C_2 \times C_2$ , we can get the more general result:

**Proposition 3.1.** *If  $n$  is divisible by two distinct odd primes, or  $n$  is a proper multiple of 4, then  $\Phi_n(x)$  is quasi-reducible. ■*

In this case, we can find explicitly the degrees of the irreducible factors of  $\Phi_n$  modulo  $p$  for a given prime  $p$ . Assume first that  $p$  does not divide  $n$ . As the Galois group of an irreducible factor is generated by the automorphism  $\alpha \mapsto \alpha^p$ , and  $\alpha^n = 1$ , we see that the order of the group is the multiplicative order of  $p$  modulo  $n$ . Since  $x^n - 1$  has no repeated roots modulo  $p$  in this case, all the irreducible factors of  $\Phi_n$  are distinct, and have the same degree.

If, on the other hand,  $p \mid n$ ,  $x^n - 1$  has repeated roots modulo  $p$ , since its derivative is 0.

In this case, we make use of the identities:

$$\Phi_m(x^p) = \begin{cases} \Phi_{mp}(x)\Phi_m(x) & \text{if } p \nmid m \\ \Phi_{mp}(x) & \text{if } p \mid m \end{cases}$$

Since, in  $\text{GF}(p)$ , we have  $f(x^p) = f(x)^p$  for any polynomial  $f$ , we get:

$$\Phi_{mp}(x) = \begin{cases} \Phi_m(x)^{p-1} & \text{if } p \nmid m \\ \Phi_m(x)^p & \text{if } p \mid m \end{cases}$$

and we can repeat the process if  $p \mid m$ . If  $n = p^k r$ , where  $p \nmid r$ , we obtain finally:

$$\Phi_n(x) = \Phi_r(x)^{\phi(p^k)}$$

where  $\Phi_r(x)$  may be further reducible.

Consider, for example, the polynomial:

$$f(x) = \Phi_{15}(x) = \frac{(x^{15} - 1)(x - 1)}{(x^3 - 1)(x^5 - 1)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

As  $U(15) = U(3) \times U(5) \cong C_2 \times C_4$ , the exponent of  $G$  is 4, and any irreducible factor of  $f_p$  has degree at most 4. If  $p \nmid 15$ , the degree of these factors is the multiplicative order of  $p$  modulo 15. For example, we have:

$$\begin{aligned} f(x) &= (x^4 + 2x^3 + 4x^2 + x + 2)(x^4 + 4x^3 + 2x^2 + x + 4) && \pmod{7} \\ &= (x^2 + 3x + 9)(x^2 + 4x + 5)(x^2 + 5x + 3)(x^2 + 9x + 4) && \pmod{11} \end{aligned}$$

and, modulo 31,  $f(x)$  splits into 8 linear factors. For  $p = 3$  and  $p = 5$ , we have:

$$\begin{aligned} f(x) &= (x^4 + x^3 + x^2 + x + 1)^2 = \Phi_5(x)^2 && \pmod{3} \\ &= (x^2 + x + 1)^4 = \Phi_3(x)^4 && \pmod{5} \end{aligned}$$

## 4 Bi-quadratic equations

We investigate now the polynomials of the form:

$$f(x) = x^4 + ux^2 + v$$

where  $v$  is a square. These polynomials have Galois group  $C_2 \times C_2$ , their roots can be expressed as  $(\pm\sqrt{a} \pm \sqrt{b})$ , where  $a$  and  $b$  need not be positive. By using different groupings of the factors, we obtain the following factorizations over  $\mathbb{C}$ :

$$\begin{aligned} f(x) &= (x^2 - a^2 - b^2 + 2\sqrt{ab})(x^2 - a^2 - b^2 - 2\sqrt{ab}) \\ &= (x^2 + 2\sqrt{a} + a - b)(x^2 - 2\sqrt{a} + a - b) \\ &= (x^2 + 2\sqrt{b} - a + b)(x^2 - 2\sqrt{b} - a + b) \end{aligned}$$

These factorizations can be used over  $\text{GF}(p)$ , provided that the required square roots exist, i.e., if the expressions under the radicals are quadratic residues. Now, if  $(k/p)$  denotes the Legendre symbol, we have:

$$(a/p)(b/p)(ab/p) = (a^2b^2/p) = +1 \text{ or } 0$$

which shows that at least one of  $a$ ,  $b$ , or  $ab$  is a quadratic residue, and we can use the corresponding factorization. Furthermore, if both  $a$  and  $b$  are quadratic residues, the roots are in  $\text{GF}(p)$  and  $f$  splits into linear factors.

Consider, for example, the polynomial:

$$f(x) = x^4 - 10x^2 + 1$$

whose roots are  $(\pm\sqrt{2} \pm \sqrt{3})$ . For  $p = 2$  and  $p = 3$ , we have the factorizations:

$$\begin{aligned} f(x) &= (x + 1)^4 && \pmod{2} \\ &= (x^2 + 1)^2 && \pmod{3} \end{aligned}$$

For the other primes, we use the theory of quadratic reciprocity to find the values of the Legendre symbols  $(2/p)$ ,  $(3/p)$  and  $(6/p)$  depending on the congruence class of  $p$  modulo 24. The results are shown in table 4.1. Using these values, we can exhibit an example of each

$p \pmod{24}$	1	5	7	11	13	17	19	23
$(2/p)$	+	-	+	-	-	+	-	+
$(3/p)$	+	-	-	+	+	-	-	+
$(6/p)$	+	+	-	-	-	-	+	+

Table 4.1: Legendre symbols  $(2/p)$ ,  $(3/p)$  and  $(6/p)$

kind of factorization:

$$\begin{aligned} f(x) &= (x^2 + 2)(x^2 + 3) && \pmod{5} \\ &= (x^2 + x + 6)(x^2 + 6x + 6) && \pmod{7} \\ &= (x^2 + x + 1)(x^2 + 10x + 1) && \pmod{11} \\ &= (x + 2)(x + 11)(x + 12)(x + 21) && \pmod{23} \end{aligned}$$

We may also mention that the cyclotomic polynomial  $\Phi_8(x) = x^4 + 1$  can also be analyzed using this technique, with  $a = 1/2$  and  $b = -1/2$ .

## 5 Non-abelian groups

A random polynomial has “usually” a non-abelian Galois group. Therefore, in this case, any normal polynomial generating the splitting field will be quasi-reducible. For example, let us consider the polynomial:

$$g(x) = x^3 + 2x^2 - x + 3 \tag{5.1}$$

The discriminant of this polynomial is  $-439$ , and the Galois group is therefore  $S_3$ . To find a normal polynomial, we compute the minimal polynomial of  $\zeta = (\alpha - \beta)$ , where  $\alpha$  and  $\beta$  are roots of  $g$ . This gives the polynomial:

$$f(x) = x^6 - 14x^4 + 49x^2 + 439 \quad (5.2)$$

with discriminant equal to  $-2^6 \cdot 5^4 \cdot 23^4 \cdot 439$ . As  $f$  has degree 6, it is a normal polynomial, and is therefore quasi-reducible, since  $S_3$  is not abelian (and therefore not cyclic). We note that, in this case, we have  $e = |G| = 6$ . Factorization modulo some small primes produces various patterns; for example:

$$\begin{aligned} f(x) &= (x^3 + x + 1)^2 && \pmod{2} \\ &= (x^2 + 1)(x^2 + x + 2)(x^2 + 2x + 2) && \pmod{3} \\ &= (x + 1)(x + 2)^2(x + 3)^2(x + 4) && \pmod{5} \\ &= (x^3 + 4x + 1)(x^3 + 4x + 10) && \pmod{11} \\ &= (x + 1)(x + 2)(x + 3)(x + 16)(x + 17)(x + 18) && \pmod{19} \\ &= (x^2 + 6)(x^2 + 13)^2 && \pmod{23} \\ &= x^2(x + 165)^2(x + 274)^2 && \pmod{439} \end{aligned}$$

We can make a few preliminary observations:

- The degrees of the factors are divisors of 6, as expected, since  $G_p$  is a subgroup of  $S_3$ .
- We never have a factor of degree 2 and a factor of degree 3 in the same factorization, since the resulting Galois group would be  $C_6$ , which is not isomorphic to a subgroup of  $S_3$ .
- There are repeated factors for the primes that divide the discriminant of  $f$ ; this corresponds to the definition of the discriminant.

Let us now analyze in more detail the structure of the possible factorizations. In what follows, we will use the following notations and conventions:

- $f(x) = x^3 + ux^2 + vx + w$  is a separable polynomial (possibly reducible) over a field  $K$ , not of characteristic 2.
- The roots of  $f$  are  $\alpha, \beta$ , and  $\gamma$ ; the discriminant is  $\Delta$ .
- The splitting field of  $f$  is  $L$ .
- By a common abuse of language, we call an element of  $L$  “rational” if it belongs to  $K$ .

**Proposition 5.1.** *With the above notations,  $L = K(\alpha, \sqrt{\Delta})$ , where  $\alpha$  is any root (possibly rational) of  $f$ .*

*Proof.* It is obvious that  $L$  contains  $\alpha$  and  $\sqrt{\Delta} = (\alpha - \beta)(\beta - \gamma)(\alpha - \gamma)$ , and therefore  $K(\alpha, \sqrt{\Delta}) \subset L$ . To show the reverse inclusion, we must prove that  $\beta \in K(\alpha, \sqrt{\Delta})$ , since  $L = K(\alpha, \beta)$ .

We have:

$$\begin{aligned} \sqrt{\Delta} &= (\alpha - \beta)(\beta - \gamma)(\alpha - \gamma) \\ &= (\beta - \gamma)(\alpha^2 - \alpha(\beta + \gamma) + \beta\gamma) \\ &= (\beta - \gamma)\theta \\ \theta &= (\alpha^2 - \alpha(\beta + \gamma) + \beta\gamma) \end{aligned}$$

We note that  $\theta \in K(\alpha)$ , since  $\beta + \gamma = -u - \alpha$  and  $\beta\gamma = v - \alpha(\beta + \gamma) = v + \alpha(u + \alpha)$ . If  $\theta = 0$ , either  $\alpha = \beta$  or  $\alpha = \gamma$  and  $\beta = u - 2\alpha$ . In either case, we have  $\beta \in K(\alpha) \subset K(\alpha, \sqrt{\Delta})$ . If  $\theta \neq 0$ , we have:

$$\beta - \gamma = \frac{\sqrt{\Delta}}{\theta} \in K(\alpha, \sqrt{\Delta})$$

and, since  $\beta + \gamma \in K(\alpha)$ , and  $\text{char}K \neq 2$ , we conclude that  $\beta \in K(\alpha, \sqrt{\Delta})$ .  $\square$

We now return to the investigation of the degrees of the irreducible factors of  $f_p$  over  $K = \text{GF}(p)$  (for odd  $p$ ) and their relation with the factors of  $g_p$ . As remarked before, the splitting field  $L$  cannot have degree 6, since the Galois group would have to be  $C_6$ , which is not a subgroup of  $S_3$ .

- If  $\Delta$  is not a quadratic residue modulo  $p$ ,  $K(\sqrt{\Delta})$  is an extension of degree 2. By the remark above, we have  $L = K(\sqrt{\Delta})$ , which means that there is at least one factor of degree 2 and no factors of degree 3.
- If  $\Delta$  is a quadratic residue,  $L = K(\alpha)$ . If  $g_p$  is irreducible,  $L$  has degree 3, and the possible degrees of the factors of  $f_p$  are  $(3, 3)$  or  $(3, 1, 1, 1)$ . If, on the other hand,  $g_p$  is reducible, it has at least one linear factor. By choosing the rational root as  $\alpha$ , we find that  $L = K$ , which means that  $f_p$  splits into 6 linear factors. This also implies that  $g_p$  splits into three linear factors.

In the above examples, we notice that the degrees of the irreducible factors of  $f_p$  are the same, which suggests the following conjecture:

**Conjecture 5.2.** *If  $f(x)$  is a quasi-reducible polynomial, the irreducible factors of  $f_p$  have the same degree.*

We know that the conjecture is true for cyclotomic and bi-quadratic polynomials with Galois group  $C_2 \times C_2$ . As we will see, the conjecture is false in general, but counter-examples are somewhat hard to find. In particular, the conjecture is true for the specific polynomial given by (5.2); this is related to the choice of  $\zeta = \alpha - \beta$  as primitive element.

In the case of a cubic polynomial over  $\mathbb{Q}$ , we can choose as primitive element any element of the splitting field that does not belong to  $\mathbb{Q}(\alpha)$ , for any root  $\alpha$ . Such an element can be expressed as a polynomial  $P(\alpha, \beta)$ , and we can independently choose the roots  $\alpha$  and  $\beta$ , as the Galois group is  $S_3$ . The 6 roots of  $f$  correspond to the 6 possible choices, and all these roots have the same minimal polynomial (which is, of course,  $f$  itself).

However, over a finite field  $\text{GF}(p)$ , this is no longer true, because the Galois group is generated by the Frobenius automorphism  $\sigma : \alpha \mapsto \alpha^p$ . Once a root  $\alpha$  has been chosen, the other roots of the corresponding irreducible factor of  $g$  can be identified individually as  $\alpha^p, \alpha^{p^2}, \dots$ . We may therefore expect that different choices of  $\beta$  could produce different results.

Before showing how this idea can be used to produce counter-examples, let us first show that the conjecture holds for the particular polynomial  $f(x)$  given by (5.2), at least for odd primes. We have already seen that  $f_p$  splits into linear factors if and only if  $g_p$  does. There are two remaining cases:

1.  $g_p$  is irreducible. In this case, the splitting field is  $\text{GF}(p^3)$ , and  $f_p(x)$  has an irreducible factor  $q_p(x)$  of degree 3. We notice that  $f_p$  is an even polynomial, because, if  $\zeta = \alpha - \beta$

is a root of  $f$ ,  $-\zeta$  is also a root. As  $q_p$  is an irreducible cubic, it contains a term  $x^3$  and a constant term, and is therefore neither odd nor even. This means that we must have  $f_p(x) = -q_p(x)q_p(-x)$ , and, if  $q_p(x)$  is irreducible, so is  $q_p(-x)$ .

2.  $g_p$  factors into a linear factor and an irreducible quadratic. In this case, the splitting field is  $\text{GF}(p^2)$ . If  $\alpha$  and  $\beta$  are the roots of the quadratic,  $\alpha - \beta$  is irrational (because  $\alpha + \beta$  is rational). If one of  $\alpha$  or  $\beta$  is the rational root,  $\alpha - \beta$  is also irrational. We may therefore conclude that all the roots of  $f_p$  are irrational, and the corresponding minimal polynomials are of degree 2, since  $f_p$  splits in  $\text{GF}(p^2)$ .

Let us now find counter-examples to conjecture 5.2. We first notice that the proof above fails for  $p = 2$ . This is related to the fact that, over  $\text{GF}(2)$ , the polynomial  $x^2 + x + 1$  is irreducible, although its discriminant is equal to 1. We start with the polynomial:

$$g(x) = x(x^2 + x + 1) + 2 = x^3 + x^2 + x + 2$$

and we compute, as before, the minimal polynomial of  $\alpha - \beta$ :

$$f(x) = x^6 + 4x^4 + 4x^2 + 83$$

Over  $\text{GF}(2)$ , we have the factorization:

$$f_2(x) = (x + 1)^2(x^2 + x + 1)^2$$

which provides a first counter-example to the conjecture.

As the case  $p = 2$  is rather special, we now look for counter-examples modulo other primes. We take  $p = 11$ , and  $g(x)$  as in (5.1);  $g_{11}$  is irreducible. If  $\alpha$  is a root of  $g_{11}$  in  $\text{GF}(11^3)$ , the other two roots are  $\alpha^{11}$  and  $\alpha^{121}$ . As  $g_{11}(\alpha) = 0$ , we obtain, by division:

$$\alpha^{11} = 4\alpha^2 + 4\alpha + 5 \tag{5.3}$$

We define the primitive element as:

$$\zeta = 4\alpha^2 + 4\alpha + 5 - \beta \tag{5.4}$$

Now, (5.4) can be taken as a definition over  $\mathbb{Q}$ , and we obtain the minimal polynomial:

$$h(x) = x^6 - 66x^5 + 1665x^4 - 22474x^3 + 199078x^2 - 1047376x + 3347465$$

which is quasi-reducible. When  $p = 11$ , if we choose  $\beta = \alpha^{11}$ , we have  $\zeta = 0$ , and the minimal polynomial of that particular root of  $f_{11}$  is  $x$ . Indeed, over  $\text{GF}(11)$ , we have the factorization:

$$h_{11}(x) = x^3(x^3 + 4x + 10)$$

which is a counter-example to conjecture 5.2, since the degrees of the irreducible factors are  $(3, 1, 1, 1)$ .

To obtain an example with a quadratic factor, we take  $p = 3$ , in which case  $g_3$  splits as:

$$g_3(x) = x(x^2 + 2x + 2)$$

We take the primitive element:

$$\zeta = \alpha^3 - \beta = 2\alpha + 1 - \beta$$

and obtain the quasi-reducible polynomial:

$$k(x) = x^6 - 2x^5 - 31x^4 + 128x^3 + 160x^2 - 1536x + 6255$$

which factors over  $\text{GF}(3)$  as:

$$k_3(x) = x^2(x^2 + 2x + 2)^2$$

where the degrees of the irreducible factors are  $(2, 2, 1, 1)$ .

In each of the counter-examples above, we find that we get a repeated factor. This is due to the fact that the number of possible inequivalent choices for the pair  $(\alpha, \beta)$  gives an upper bound on the number of *distinct* irreducible factors. For example, if  $g$  is irreducible, the choice of  $\alpha$  is arbitrary, and there are two possible choices for  $\beta$ , and therefore there can be at most two distinct irreducible factors, corresponding to the minimal polynomials of the corresponding  $\zeta$ . If  $g$  factors as  $(2, 1)$ , there are three possible choices, depending on which root  $(\alpha, \beta, \text{ or } \gamma)$  is taken as the rational root. As the factorization of (5.2) modulo 5 shows, this is only an upper bound.

## References

- [1] Paul M. Cohn. *Algebra*, volume 2. Wiley, second edition, 1989. ISBN 0-471-92235-8.