GALOIS THEORY TOPIC VI
IRREDUCIBILITY CRITERIA

PAUL L. BAILEY

Abstract. We now refocus on polynomials over subfields of $\mathbb{C}$, with emphasis on polynomials over $\mathbb{Q}$; we develop several criteria to help us determine when such polynomials are irreducible.

1. Polynomials over $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Q}$

1.1. **Polynomials over $\mathbb{C}$.** First we consider polynomials with complex coefficients, and how to factor them over $\mathbb{C}$.

Theorem 1. (Fundamental Theorem of Algebra)
If $f \in \mathbb{C}[x]$, then f has a root in $\mathbb{C}$.

Proof. This was suspected since the 1500's when complex number first came into use, but was not proved until 1800, when Gauss did so in his doctoral dissertation. The proof is deep, requiring advanced techniques of complex analysis or abstract field theory, and is not within our reach. We accept this statement for the purposes of orientation, but do not draw any conclusion from it after this section. □

Proposition 1. *If $f \in \mathbb{C}[x]$ with $\deg(f) = n$, then f is the product of exactly n linearly factors.*

Proof. By the Fundamental Theorem of Algebra, f has a root in $\mathbb{C}$. Let $a \in \mathbb{C}$ be a root of f so that $f = (x - a)q$ for some q with $\deg(q) = n - 1$. By induction, q has exactly $n - 1$ linear factors. Thus f has exactly n linear factors. □

Date: October 18, 2006.

1.2. **Polynomials over $\mathbb{R}$.** Next we consider polynomials over $\mathbb{R}$, and how to factor them over $\mathbb{R}$.

Proposition 2. *Let $f \in \mathbb{R}[x]$ and let $w \in \mathbb{C}$ be a root of f. Then $f(\overline{w}) = 0$, where $\overline{w}$ denotes the complex conjugate of w.*

Proof. Let $z = a + bi$ be an arbitrary complex number. Then $\overline{z} = a - bi$. Suppose that $w = c + di$; then

$$\overline{z + w} = \overline{(a+c) + (b+d)i} = (a+c) - (b+d)i = (a - bi) + (c - di) = \overline{z} + \overline{w},$$

and

$$\overline{z \cdot w} = \overline{(ac - bd) + (ad + bd)i} = (ac - bd) - (ad + bd)i = \overline{z} \cdot \overline{w}.$$

Moreover, if $a \in \mathbb{R}$, then $\overline{a} = a$. The corollary follows from these properties of complex conjugation, as follows.

Let $f(z) = \sum_{i=0}^{n} a_i x^i$, where $a_i \in \mathbb{R}$ for all i. No Then for $w \in \mathbb{C}$, we have

$$\overline{f(w)} = \overline{\sum_{i=0}^{n} a_i w^i} = \sum_{i=0}^{n} \overline{a_i}\overline{w^i} = \sum_{i=0}^{n} a_i \overline{w}^i = f(\overline{w}).$$

Thus $f(w) = f(\overline{w})$, so if $f(w) = 0$, we have $f(\overline{w}) = 0$. □

Proposition 3. *Let $f \in \mathbb{R}[x]$. Then f factors into a product of linear and irreducible (over $\mathbb{R}$) quadratic polynomials.*

Proof. By the previous proposition, if $w \in \mathbb{C} \setminus \mathbb{R}$ is a complex root of f, then so is $\overline{w}$. Thus $(z - w)$ and $(z - \overline{w})$ are factors of f over $\mathbb{C}$, but not over $\mathbb{R}$. However, $(z - w)(z - \overline{w}) = z^2 - (w + \overline{w})z + w\overline{w} = z^2 - 2\Re(w) + |w|^2$ is a quadratic factor of f with coefficients in $\mathbb{R}$. So, the linear factors of f over $\mathbb{R}$ are of the form $(z - u)$, where $u \in \mathbb{R}$ is a real roots, and the irreducible quadratic factors are of the form $(z - w)(z - \overline{w})$, where $w \in \mathbb{C}$ is a nonreal complex root. This accounts for all of the roots, and so gives a complete factorization. □

1.3. **Polynomials over $\mathbb{Q}$.** Finally, we mention how one can find linear factors over $\mathbb{Q}$ of a polynomial with rational coefficients.

Given a polynomial $f \in \mathbb{Q}[x]$, we note that the coefficients are rational numbers, and we may assume that the coefficients are in lowest form. Let $F \in \mathbb{Z}$ be the least common multiple of the coefficients of the polynomial, and set $g = Ff$; then g is a polynomial with integer coefficients, and the roots of g are the same as those of f. Thus if we wish to understand the rational roots of polynomials with rational coefficients, it suffices to consider polynomials with integer coefficients. Towards this end, we have the following proposition. If we multiply f by the least common multiple of the denominators of the coefficients

Proposition 4. (Rational Roots Theorem)
Let $f \in \mathbb{Z}[x]$, so that $f(x) = a_n x^n + \cdots + a_1 x + a_0$, where $a_i \in \mathbb{Z}$. Suppose that $\frac{p}{q}$ is a rational zero of f, where $\gcd(p, q) = 1$. Then $p \mid a_0$ and $q \mid a_n$.

Proof. We have $f(\frac{p}{q}) = 0$; multiply this equation by q^n to obtain

$$a_n p^n + a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \cdots + a_2 p^2 q^{n-2} + a_1 p q^{n-1} + a_0 q^n = 0.$$

Solve this for $a_0 q^n$ to obtain

$$a_0 q^n = p(-1)(a_n p^{n-1} + a_{n-1} p^{n-2} q + \cdots + a_1 q^{n-1}).$$

Thus $p \mid a_0 q^n$; by a lemma from our study of integer arithmetic, since p and q are relatively prime, we conclude that $p \mid a_0$.

Similarly, solve the original equation for $a_n p^n$ to obtain

$$a_n p^n = q(-1)(a_{n-1} p^{n-1} + \cdots + a_1 p q^{n-2}) + a_0 q^{n-1};$$

in this case, $q \mid a_n p^n$, so $q \mid a_n$. □

2. Low Degree Irreducibility Criteria

Proposition 5. (Low Degree Irreducibility Criterion)
Let F be a field and let $f \in F[x]$. If $2 \leq \deg(f) \leq 3$, then f is irreducible over F if and only if f does not have a root in F.

Proof. This, of course, is the same as saying that f reduces over F if and only if f has a root in F.

If $f = gh$ is a proper factorization over F, then $\deg)(g) < 3$, $\deg(h) < 3$, and $\deg(g) + \deg(h) = \deg(f) \leq 3$. Thus either $\deg(g) = 1$ or $\deg(h) = 1$; without loss of generality, suppose $\deg(g) = 1$. Then $g(x) = ax + b$, where $a, b \in F$. Then $\frac{-b}{a}$ is a root of g, and hence is a root of f.

In the other hand, if $a \in F$ and $f(a) = 0$, then $(x - a)$ is factor of f, as we have previously seen. □

To apply the low degree irreducibility criterion to a polynomial with integer coefficients, one may use the rational roots theorem to demonstrate that no rational root is possible for a quadratic or cubic polynomial. We summarize this as follows.

Proposition 6. *Let $f \in \mathbb{Z}[x]$ be a quadratic or cubic polynomial. If*

$$p, q \in \mathbb{Z}, p \mid \mathrm{CC}(f), q \mid \mathrm{LC}(f) \quad \Rightarrow \quad f(\frac{p}{q}) \neq 0,$$

then f is irreducible.

Example 1. Show the $f(x) = x^3 - 2x + 9$ is irreducible over $\mathbb{Q}$.

Solution. Using synthetic division, we evaluate f at every positive and negative divisor of 9, and find that $f(1) = 8$, $f(-1) = 10$, $f(3) = 30$, $f(-3) = -12$, $f(9) = 720$, and $f(-9) = -702$. Since none of these are zero, f has no rational roots, and since f is cubic, it must be irreducible. □

3. Modular Irreducibility Criterion

Recall the function $\xi_n : \mathbb{Z} \to \mathbb{Z}_n$ given by reduction modulo n, that is, by taking the remainder upon division by n. This function has the properties that $\xi(a+b) = \xi(a) + \xi(b)$ and $\xi(ab) = \xi(a)\xi(b)$.

Let $p \in \mathbb{Z}$ be prime, and extend the residue map ξ_p to a function from the ring of polynomials with integer coefficients to the ring of polynomials over $\mathbb{Z}_p$ by

$$\xi_n : \mathbb{Z}[x] \to \mathbb{Z}_p[x] \quad \text{given by} \quad \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} \overline{a_i} x^i;$$

that is, we reduce each coefficient modulo n.

Proposition 7. *Let $p \in \mathbb{Z}$ be prime, and let $f, g \in \mathbb{Z}[x]$. Then*

(a) *$\xi_p(f+g) = \xi_p(f) + \xi_p(g)$;*
(b) *$\xi_p(f)\xi_p(g)$.*

Proof. Two functions are equal if they are equal at each point in the domain. Thus let $x \in \mathbb{Z}_n$; then $\overline{x} = x$, and since f is a polynomial and BAR splits on sums and products, $\overline{f(x)} = \overline{f}(\overline{x}) = \overline{f}(x)$. Moreover,

$$\overline{f(x) + g(x)} = \overline{f(x)} + \overline{g(x)} = \overline{f}(x) + \overline{g}(x);$$

since x is arbitrary, this is true for all x, giving **(a)**. Also **(b)** follows analogously. □

Proposition 8. *Let $p \in \mathbb{Z}$ be prime, and let $f \in \mathbb{Z}[x]$. Then* $\deg(f) = \deg(\overline{f})$ *if and only if p does not divides* $\mathrm{LC}(f)$.

Proof. This is clear from the definition. □

Proposition 9. (Modular Irreducibility Criterion)
Let $f \in \mathbb{Z}[x]$ and let $p \in \mathbb{Z}$ be a prime which does not divide the leading coefficient of f. Let $\overline{f} \in \mathbb{Z}_p[x]$ denote the polynomial obtained by reduction modulo p. If $\overline{f}$ is irreducible in $\mathbb{Z}_p[x]$, then f is irreducible in $\mathbb{Z}[x]$.

Proof. Suppose f reduces over $\mathbb{Z}$; then $f = gh$ where $g, h \in \mathbb{Z}[x]$ with $\deg(g) < \deg(f)$ and $\deg(h) < \deg(f)$. We know that $\mathrm{LC}(f) = \mathrm{LC}(g)\,\mathrm{LC}(h)$, and since p does not divide $\mathrm{LC}(f)$, then p cannot divide $\mathrm{LC}(g)$ or $\mathrm{LC}(h)$.

Reduction modulo p gives $\overline{f} = \overline{g}\overline{h}$, preserving the degrees of each polynomial, and giving a proper factorization in $\mathbb{Z}_p[x]$. □

Example 2. Show that $f(x) = 33x^3 - 154x^2 + 343x + 130$ is irreducible over $\mathbb{Z}$.

Solution. We could attempt to analyze this via the rational roots theorem, but since 130 has 7 positive divisors and 33 has 4 positive divisors, this would require $2 \cdot 4 \cdot 7 = 56$ evaluations. However, if we notice that 7 divides 154 and 343, we reduce the polynomial modulo 7 to obtain

$$\overline{f}(x) = -2x^3 - 10 = x^3 - 5.$$

The only cubes modulo 7 are 1 and $6 = -1$, so $\overline{f}$ is irreducible over $\mathbb{Z}_p$, and consequently, f is irreducible over $\mathbb{Z}$. □

4. Gauss' Lemmas

Definition 1. Let $f \in \mathbb{Z}[x]$. Then *content* of f is the greatest common divisor of the coefficients of f, and is denoted $\operatorname{con}(f)$.

We say that f is *primitive* if $\operatorname{con}(f) = 1$.

Example 3. The content of $f(x) = 14x^5 - 49x^3 + 210x - 63$ is $\operatorname{con}(f) = 7$, so f is not primitive. However, the content of $g(x) = 2x^5 - 7x^3 + 30x - 9$ is $\operatorname{con}(f) = 1$, so g is primitive.

Note that if $F = \operatorname{con}(f)$, then $\frac{1}{F}\operatorname{con}(f)$ has integer coefficients and is primitive. Also note that if f is primitive and $C \in \mathbb{Z}$ is positive, then $\operatorname{con}(Cf) = C$.

Proposition 10. (Gauss' Lemma Form I)
The product of primitive polynomials is primitive.

Proof. Let $f, g, h \in \mathbb{Z}[x]$ with $f = gh$, and suppose that g and h are primitive but that f is not. Let $F = \operatorname{con}(f)$, and let p be a prime which divides F. Reduction modulo p gives

$$\overline{f} = \overline{g}\overline{h}.$$

Since p divides every coefficient of f, these coefficients are congruent to zero modulo p, so $\overline{f} = 0$, the zero polynomial in $\mathbb{Z}_p[x]$. However, since g and h are primitive, their reductive modulo p is nonzero, so $\overline{g}\overline{h}$ is nonzero, a contradiction. □

Proposition 11. (Gauss Lemma Form II)
Let $f \in \mathbb{Z}[x]$, and suppose that there exist $g, h \in \mathbb{Q}[x]$ such that $f = gh$. Then there exist $g_1, h_1 \in \mathbb{Z}[x]$ such that $f = g_1h_1$.

Proof. First assume that f is primitive. Write the rational coefficients of g and h in lowest form, and let G and H be the least common multiples of the denominators of the coefficients of g and h, respectively. Then Gg and Hh have integer coefficients, and $GHf = (Gg)(Hh)$.

Let $C = \operatorname{con}(Gg)$ and $D = \operatorname{con}(Hh)$, and set $g_1 = \frac{G}{C}g$ and $h_1 = \frac{H}{D}h$. Now g_1 and h_1 are primitive, and $GHf = CDg_1h_1$. By Gauss' Lemma Form I, g_1h_1 is primitive. Thus, since f is also primitive,

$$GH = \operatorname{con}(GHf) = \operatorname{con}(CDg_1h_1) = CD.$$

Dividing this common quantity from both sides of $GHf = CDg_1h_1$ gives $f = g_1h_1$, so f reduces into a product of polynomials with integer coefficients.

If the original f is not primitive, let $F = \operatorname{con}(f)$ so that $\frac{1}{F}f$ is primitive. Then $\frac{f}{F} = \frac{g}{F}h$, and applying the results of the previous paragraph, Then $\frac{1}{F}f = g_1h_1$ for some $g_1, h_1 \in \mathbb{Z}[x]$. Now $f = (Fg_1)h_1$ factors f as a product of polynomials with integer coefficients. □

5. Eisenstein's Criterion

Proposition 12. (Eisenstein's Criterion)
Let $f \in \mathbb{Z}[x]$, where $f(x) = \sum_{k=0}^{n} a_k x^k$. Suppose that

- **(a)** *p does not divides a_n;*
- **(b)** *p divides a_k for $k < n$;*
- **(c)** *p^2 does not divide a_0.*

Then f is irreducible over $\mathbb{Q}$.

Proof. Let $g(x) = \sum_{k=0}^{r} b_k x^k$ and $h(x) = \sum_{k=0}^{s} c_k x^k$, and suppose (by way of contradiction) that $f = gh$ where $r > 0$, $s > 0$, and $n = r + s$. By Gauss' Lemma, we may assume that g and h have integer coefficients.

Then

$$a_t = \sum_{i+j=t} b_i c_j.$$

Now $a_0 = b_0 c_0$, and p^2 does not divide a_0, so p does not divide b_0 or p does not divide c_0; without loss of generality, assume p does not divide c_0; we know that p divides b_0.

Also, $a_k = b_r c_s$ is not divisible by p, so neither are b_r nor c_s. Let t be the smallest integer such that p does not divide b_t; then p divides $b_0, b_1, \dots b_{t-1}$. We note that $t < n$.

Consider $a_t = b_0 c_t + b_1 c_{t-1} + \cdots + b_{t-1} c_1 + b_t c_0$; we have

$$b_t c_0 = a_t - (b_0 c_t + b_1 c_{t-1} + \cdots b_{t-1} c_1).$$

Since p divides every summand on the right hand side, p divides the sum. But p does not divide b_t, nor does p divide c_0, so p does not divide the product $b_t c_0$. This contradiction completes the proof. □

Example 4. Show that $f(x) = 2x^5 + 21x^4 - 42x^3 + 245x + 700$ is irreducible over $\mathbb{Q}$.

Solution. Let $p = 7$. Then p does not divide the leading coefficient of f (which is 2), but does divide every other coefficient. Also, $p^2 = 49$ does not divide the constant coefficient (which is 700). Thus, by Eisenstein's criterion, f is irreducible over $\mathbb{Q}$. □

6. Cyclotomic Polynomials

Definition 2. Let p be a prime integer. The p^{th} *cyclotomic polynomial* is

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1.$$

Note that $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \dots + x + 1)$, which can be seen by multiplying out the right hand side. Therefore, $(x-1)$ divides $x^n - 1$, and

$$\frac{x^n - 1}{x - 1} = \sum_{k=0}^{n-1} x^k.$$

Each of the n^{th} complex roots of unity is a root of the polynomial equation $x^n - 1 = 0$, and there are exactly n of them. Thus x^{n-1} is the product of all of the distinct linear terms of the form $(x - \zeta)$, where $\zeta^n = 1$. In particular, the roots of $\Phi_p(x)$ are exactly the primitive p^{th} roots of unity. This accounts for our interest in this cyclotomic polynomial.

Proposition 13. *If p is prime, then $\Phi_p(x)$ is irreducible over $\mathbb{Q}$.*

To prove this, we perform a "linear change of variable"; we state this as a lemma.

Lemma 1. (Linear Change of Variable Lemma)
Let F be a field and let $f \in F[x]$. Let $a, b \in F$ with $a \neq 0$. If $f(ax+b)$ is irreducible over F, then $f(x)$ is irreducible over F.

Proof of Lemma. First we note that for any polynomials $g, h \in F[x]$, the composition of $(g \circ h)(x) = g(h(x))$ is another polynomial in $F[x]$, and in fact, $\deg(g \circ h) = \deg(g)\deg(h)$. In particular, if the degree of h is one, we obtain a polynomial in x of the same degree.

Suppose that f is reducible over F; and let $f_1(x) \in F[x]$ be given by $f_1(x) = f(ax+b)$. We wish to see that f_1 is reducible over F.

Since f is reducible over F, then $f = gh$ for some $g, h \in F[x]$. That is, $f(x) = g(x)h(x)$, and this holds for every $x \in F$. Thus $f(ax+b) = g(ax+b)h(ax+b)$, with $g(ax+b)$ and $h(ax+b)$ being polynomials in x, whose coefficients are in F, of the same degree as g and h. In particular, with $g_1(x) = g(ax+b)$ and $h_1(x) = h(ax+b)$, we see that $f_1(x) = g_1(x)h_1(x)$ is a proper factorization of f_1; thus f_1 is reducible over F. □

Proof of Proposition. By the preceding lemma, it suffices to show that $\Phi_p(x+1)$ is irreducible. Using the binomial expansion of $(x+1)^p$, we have

$$\begin{aligned}\Phi_p(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{p-1}x + 1 - 1}{x} \\ &= x^{p-1} + \binom{p}{1}x^{p-1} + \dots \binom{p}{p-2}x + \binom{p}{p-1}.\end{aligned}$$

Now p divides $\binom{p}{k}$ for $1 \leq k \leq p-1$, and $\binom{p}{p-1} = p$ is not divisible by p^2. Thus $\Phi_p(x+1)$ satisfies the hypothesis of Eisenstein's criterion, and so is irreducible. □

Department of Mathematics and CSci, Southern Arkansas University
E-mail address: plbailey@saumag.edu