IRREDUCIBILITY TESTS IN $\mathbf{Q}[T]$

KEITH CONRAD

1. Introduction

For a general field F there is no simple way to determine if an arbitrary polynomial in $F[T]$ is irreducible. Here we will focus on the case $F = \mathbf{Q}$ and describe two useful irreducibility tests in $\mathbf{Q}[T]$ for *monic polynomials in* $\mathbf{Z}[T]$. Let

$$f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0 \in \mathbf{Z}[T].$$

The two tests are

- Reduction mod p: for a prime p, reducing coefficients of $f(T)$ modulo p leads to
$$\overline{f}(T) = T^n + \overline{a}_{n-1}T^{n-1} + \cdots + \overline{a}_0 \in (\mathbf{Z}/p\mathbf{Z})[T].$$
If $\overline{f}(T)$ is irreducible in $(\mathbf{Z}/p\mathbf{Z})[T]$ for *some* p, then f is irreducible in $\mathbf{Q}[T]$.
- Eisenstein criterion: call $f(T)$ *Eisenstein* at p if $p \mid a_i$ for all i and $p^2 \nmid a_0$. If f is Eisenstein for *some* p, then f is irreducible in $\mathbf{Q}[T]$.

These tests each depend on a choice of a prime number, but they use the prime number in different ways.

Example 1.1. The polynomial T^3+T+1 is irreducible in $(\mathbf{Z}/2\mathbf{Z})[T]$, so every monic cubic in $\mathbf{Z}[T]$ that reduces modulo 2 to T^3+T+1 is irreducible in $\mathbf{Q}[T]$, such as T^3-4T^2+3T+1.

Example 1.2. The polynomial $T^6 + T + 1$ is irreducible in $\mathbf{Q}[T]$ because it is irreducible in $(\mathbf{Z}/2\mathbf{Z})[T]$. To show irreducibility in $(\mathbf{Z}/2\mathbf{Z})[T]$, we just have to check it is not divisible by any irreducibles of degree 1, 2, or 3 in $(\mathbf{Z}/2\mathbf{Z})[T]$: there are two irreducibles of degree 1 (T and $T + 1$), one irreducible of degree 2 ($T^2 + T + 1$), and two irreducibles of degree 3 ($T^3 + T + 1$ and $T^3 + T^2 + 1$). This leaves us with a finite amount of computation, which you should go through yourself.

Example 1.3. Let $f(T) = T^3 - 2$. Then

$$\begin{aligned} f(T) &\equiv T^3 \bmod 2, \\ f(T) &\equiv T^3 + 1 \bmod 3 \\ &\equiv (T+1)(T^2 - T + 1) \bmod 3, \\ f(T) &\equiv (T-3)(T^2 + 3T + 9) \bmod 5, \end{aligned}$$

so f is reducible mod p for $p = 2, 3, 5$. However $f(T)$ mod 7 is irreducible since f mod 7 has degree 3 in $(\mathbf{Z}/7\mathbf{Z})[T]$ and has no root in $\mathbf{Z}/7\mathbf{Z}$: that is a finite check since $\mathbf{Z}/7\mathbf{Z}$ is finite. By the reduction mod p test at $p = 7$, $T^3 - 2$ is irreducible in $\mathbf{Q}[T]$.

Remark 1.4. There are monic polynomials in $\mathbf{Z}[T]$ that are irreducible in $\mathbf{Q}[T]$ but are reducible mod p for all p, *e.g.*, $T^4 - 10T^2 + 1$. So the reduction mod p test does not always apply.

Example 1.5. $T^3 - 2$ is Eisenstein at 2, so it's irreducible in $\mathbf{Q}[T]$. This is a much easier method for $T^3 - 2$ than reduction mod p (Example 1.3).

Example 1.6. $T^n - 2$ is Eisenstein at 2 for any $n \geq 1$, so it is irreducible in $\mathbf{Q}[T]$.

The usefulness of the Eisenstein criterion is that it lets us *create* irreducibles in $\mathbf{Q}[T]$ of any degree we wish. (Note $T - 2$ is Eisenstein at 2: the test could be used in degree 1, but it is not necessary since all linear polynomials over a field are irreducible.)

Example 1.7. An Eisenstein polynomial at 3 is $T^{19} + 6T^{10} - 9T^4 + 75$.

2. Gauss' Lemma

To prove the reduction mod p test and the Eisenstein criterion, we will prove the polynomial in each test can't be decomposed into lower-degree factors in $\mathbf{Z}[T]$. How come that implies irreducibility in $\mathbf{Q}[T]$? For comparison, $T^2 + 1$ is irreducible in $\mathbf{R}[T]$ but if we enlarge $\mathbf{R}$ to $\mathbf{C}$ then $T^2 + 1 = (T + i)(T - i)$ in $\mathbf{C}[T]$ and the polynomial becomes reducible. Passing from $\mathbf{Z}[T]$ to $\mathbf{Q}[T]$ never turns irreducibility into reducibility. This is traditionally called Gauss' lemma.

Theorem 2.1 (Gauss)**.** *If $f(T) \in \mathbf{Z}[T]$ is monic and $f(T) = g(T)h(T)$ in $\mathbf{Q}[T]$ where $\deg g < \deg f$ and $\deg h < \deg f$ then we can write $f(T) = g_1(T)h_1(T)$ in $\mathbf{Z}[T]$, where $g_1(T)$ and $h_1(T)$ are scalar multiples of $g(T)$ and $h(T)$, respectively; in particular, $\deg g_1(T) = \deg g(T) < \deg f(T)$ and $\deg h_1(T) = \deg h(T) < \deg f(T)$.*

Therefore if a monic polynomial in $\mathbf{Z}[T]$ can't be written as a product of lower-degree polynomials in $\mathbf{Z}[T]$, it is irreducible in $\mathbf{Q}[T]$.

As an example, $T^2 - 1$ in $\mathbf{Q}[T]$ is $((4/3)T - 4/3)((3/4)T + 3/4)$, having linear factors, and in $\mathbf{Z}[T]$ it is $(T + 1)(T - 1)$, also having linear factors.

Proof. **Step 1**: Use common denominators to factor a scalar multiple of $f(T)$ in $\mathbf{Z}[T]$.

Let d and e be common denominators of the coefficients of $g(T)$ and $h(T)$, respectively, so $\boxed{g(T) = g_0(T)/d \text{ and } h(T) = h_0(T)/e}$ where $g_0(T)$ and $h_0(T)$ are both in $\mathbf{Z}[T]$. Thus

$$f(T) = g(T)h(T) = \frac{g_0(T)}{d}\frac{h_0(T)}{e} \Longrightarrow def(T) = g_0(T)h_0(T).$$

This last equation takes place in $\mathbf{Z}[T]$.

Step 2: Use greatest common divisors to get factors of $f(T)$ whose coefficients are relatively prime.

Factor out the greatest common divisor of the coefficients of $g_0(T)$ and of the coefficients of $h_0(T)$: $\boxed{g_0(T) = ag_1(T) \text{ and } h_0(T) = bh_1(T)}$ where $a, b \in \mathbf{Z}^+$, the coefficients of $g_1(T)$ are relatively prime, and the coefficients of $h_1(T)$ are relatively prime. Then

$$def(T) = g_0(T)h_0(T) = abg_1(T)h_1(T). \tag{2.1}$$

Step 3: Obtain a factorization of $f(T)$ in $\mathbf{Z}[T]$.

We will show $de = ab$, so canceling this (nonzero) factor from both sides gives us $f(T) = g_1(T)h_1(T)$ in $\mathbf{Z}[T]$ where $g_1(T) = g_0(T)/a = (d/a)g(T)$ and $h_1(T) = h_0(T)/b = (e/b)h(T)$ are scalar multiples of $g(T)$ and $h(T)$.

Since $f(T)$ is monic, looking at the leading coefficient on both sides of (2.1) we get

$$de = ab(\text{lead } g_1)(\text{lead } h_1) \quad \text{in } \mathbf{Z},$$

so $ab \mid de$. Let $c = de/ab \in \mathbf{Z}^+$, so $c \geq 1$ and (2.1) implies

$$cf(T) = g_1(T)h_1(T). \tag{2.2}$$

If $c > 1$ then it has a prime factor, say p. Reduce both sides of (2.2) modulo p: this turns (2.2) into $0 = \overline{g_1}(T)\overline{h_1}(T)$ in $(\mathbf{Z}/p\mathbf{Z})[T]$. Since $(\mathbf{Z}/p\mathbf{Z})[T]$ is an integral domain, one of $\overline{g_1}(T)$ or $\overline{h_1}(T)$ is 0, which is another way of saying all the coefficients of $g_1(T)$ are divisible by p or all the coefficients of $h_1(T)$ are divisible by p. Neither is possible, since the coefficients of $g_1(T)$ are relatively prime and the coefficients of $h_1(T)$ are relatively prime. Therefore c has no prime factor, so $c = 1$ and $f(T) = g_1(T)h_1(T)$ is a factorization of $f(T)$ in $\mathbf{Z}[T]$ where the factors $g_1(T)$ and $h_1(T)$ are scalar multiples of $g(T)$ and $h(T)$. □

A good way to think about the later part of this proof is that we applied the reduction mod p homomorphism to turn an equation in $\mathbf{Z}[T]$ into an equation in $(\mathbf{Z}/p\mathbf{Z})[T]$ for a suitably chosen prime p. We will apply this same idea in the proofs of both the reduction mod p test and the Eisenstein criterion.

3. Reduction mod p

Theorem 3.1. *If $f(T) \in \mathbf{Z}[T]$ is monic and there is a prime p such that $\overline{f}(T)$ is irreducible in $(\mathbf{Z}/p\mathbf{Z})[T]$ then $f(T)$ is irreducible in $\mathbf{Q}[T]$.*

Proof. By Gauss' lemma, to prove $f(T)$ is irreducible in $\mathbf{Q}[T]$ it suffices to show we can't write $f(T)$ as a product of lower-degree factors in $\mathbf{Z}[T]$.

Assume $f = gh$ for some $g, h \in \mathbf{Z}[T]$ with $\deg g < \deg f$ and $\deg h < \deg f$. We will get a contradiction from this.

Looking at the leading coefficients on both sides of $f = gh$ we have $1 = (\text{lead } g)(\text{lead } h)$ in $\mathbf{Z}$, so g and h both have leading coefficient 1 or both have leading coefficient -1. Therefore, after changing the signs on g and h if necessary, we can assume g and h are both monic in $\mathbf{Z}[T]$. Reduction mod p is a ring homomorphism $\mathbf{Z}[T] \to (\mathbf{Z}/p\mathbf{Z})[T]$, so it turns the equation $f = gh$ in $\mathbf{Z}[T]$ into $\overline{f} = \overline{g}\overline{h}$ in $(\mathbf{Z}/p\mathbf{Z})[T]$. Since $\overline{f}$ is irreducible, one of $\overline{g}$ or $\overline{h}$ has degree 0 and the other has degree equal to that of $\overline{f}$. Because f, g and h are all monic,

$$\begin{aligned} \deg \overline{f} &= \deg f, \\ \deg \overline{g} &= \deg g, \\ \deg \overline{h} &= \deg h. \end{aligned}$$

Therefore one of g or h has degree equal to the degree of f, but this contradicts g and h both having degree less than $\deg f$. □

4. The Eisenstein criterion

Theorem 4.1. *If $f(T) \in \mathbf{Z}[T]$ is monic and Eisenstein at a prime p then $f(T)$ is irreducible in $\mathbf{Q}[T]$.*

Proof. By Gauss' lemma it suffices, as in the proof of the reduction mod p test, to work in $\mathbf{Z}[T]$: assume $f = gh$ for some $g, h \in \mathbf{Z}[T]$ with $\deg g < \deg f$ and $\deg h < \deg f$ and get a contradiction. As in the proof of the reduction mod p test, we can assume g and h are both monic.

Write

$$f(T) = T^n + a_{n-1}T^{n-1} + \cdots a_1T + a_0 \in \mathbf{Z}[T]$$

so $p \mid a_i$ for all i and $p^2 \nmid a_0$. Passing from $\mathbf{Z}[T]$ to $(\mathbf{Z}/p\mathbf{Z})[T]$ by reduction mod p, the equation $f = gh$ implies $\overline{f} = \overline{g}\overline{h}$ in $(\mathbf{Z}/p\mathbf{Z})[T]$, so $T^n = \overline{g}\overline{h}$ in $(\mathbf{Z}/p\mathbf{Z})[T]$, and $\overline{g}$ and $\overline{h}$ are monic since g and h are monic. Since T is irreducible in $(\mathbf{Z}/p\mathbf{Z})[T]$, unique factorization in $(\mathbf{Z}/p\mathbf{Z})[T]$ tells us the only monic factors of T^n in $(\mathbf{Z}/p\mathbf{Z})[T]$ are powers of T, so $\overline{g} = T^r$ and $\overline{h} = T^s$ where

$$r = \deg \overline{g} = \deg g > 0 \qquad \text{and} \qquad s = \deg \overline{h} = \deg h > 0.$$

Saying $\overline{g} = T^r$ and $\overline{h} = T^s$ means g and h have all of their non-leading coefficients divisible by p. So from $r, s > 0$ we see $g(0)$ and $h(0)$ are divisible by p. Thus

$$a_0 = f(0) = g(0)h(0) \equiv 0 \bmod p^2,$$

which is a contradiction of the Eisenstein condition. □

Remark 4.2. The reduction mod p test and the Eisenstein criterion can be extended to cover $f(T)$ in $\mathbf{Z}[T]$ that are not necessarily monic by adding the condition that the leading coefficient of $f(T)$ is not divisible by the prime being used (automatic if $f(T)$ is monic).

(i) (Reduction mod p) If $f(T)$ has leading coefficient *not divisible by a prime* p and $\overline{f}(T)$ is irreducible in $(\mathbf{Z}/p\mathbf{Z})[T]$ then $f(T)$ is irreducible in $\mathbf{Q}[T]$. For example, $5T^4 - T + 4$ is irreducible in $\mathbf{Q}[T]$ since it is irreducible mod 3 (even though the reduction mod 3 is not monic).

(ii) (Eisenstein) Call a non-constant $f(T)$ in $\mathbf{Z}[T]$ Eisenstein at a prime p if *its leading coefficient is not divisible by* p, all lower-degree coefficients are divisible by p, and the constant term is not divisible by p^2. For example, $3T^4 - 10T^2 + 15$ is Eisenstein at 5. The Eisenstein criterion says that every nonconstant polynomial that is Eisenstein at some prime is irreducible in $\mathbf{Q}[T]$.

The proofs above can be modified to apply to non-monic $f(T)$ by first proving a version of Gauss' lemma that applies to non-monic polynomials in $\mathbf{Z}[T]$. See the appendix.

5. Enough prime values implies irreducibility

The polynomial $T^2 + 1$ is irreducible in $\mathbf{Z}[T]$, but that doesn't mean its values at integers have to be prime numbers: $a^2 + 1$ is composite for all odd $a \geq 3$ since $m^2 + 1$ is even and greater than 2. However, $a^2 + 1$ *is* prime for many values of a, such as $a = 1, 2, 4, 6$, and 10. It turns out if a polynomial in $\mathbf{Z}[T]$ takes enough prime values that proves its irreducibility!

Theorem 5.1. *If $f(T) \in \mathbf{Z}[T]$ is primitive of degree $d \geq 1$ and there are at least $2d + 1$ different integers a such that $|f(a)|$ is 1 or a prime number then $f(T)$ is irreducible in $\mathbf{Q}[T]$.*

Proof. By Gauss' lemma it suffices to prove $f(T)$ is irreducible in $\mathbf{Z}[T]$ to know it is irreducible in $\mathbf{Q}[T]$. Suppose $f(T) = g(T)h(T)$ in $\mathbf{Z}[T]$ where $\deg g < \deg f$ and $\deg h < \deg f$. Then $f(a) = g(a)h(a)$ for all $a \in \mathbf{Z}$. If $|f(a)|$ is 1 or a prime number then $g(a) = \pm 1$ or $h(a) = \pm 1$. Since $g(T)$ assumes each value on $\mathbf{Z}$ at most $\deg g$ times and $h(T)$ assumes each value on $\mathbf{Z}$ at most $\deg h$ times, the number of integers a such that $g(a) = \pm 1$ or $h(a) = \pm 1$ is at most $2 \deg g + 2 \deg h = 2 \deg f = 2d$. So if $|f(a)|$ is 1 or a prime number $2d + 1$ times then we have a contradiction, and thus $f(T)$ is irreducible in $\mathbf{Q}[T]$. □

Example 5.2. To show $T^4 - 10T^2 + 1$ is irreducible in $\mathbf{Q}[T]$, we have $|a^4 - 10a^2 + 1| = 1$ or a prime number at $a = 0, \pm 2, \pm 4, \pm 6, \pm 8$, which is $2 \cdot 4 + 1 = 9$ values.

Remark 5.3. A discussion of how many prime values (up to sign) a reducible polynomial in $\mathbf{Z}[T]$ can have is in [2, Theorem 1].

Theorem 5.1, like the reduction mod p test and Eisenstein criterion, it is not always directly applicable to prove irreducbility. For example, $T^2 + T + 4$ is irreducible but takes only even values when T runs over the integers and is never ± 2. There is a conjecture, due to Bunyakovsky, that describes when a polynomial in $\mathbf{Z}[T]$ should take prime values infinitely often, and a change of variables can convert any irreducible polynomial to a form where Bunyakovsky's conjecture is expected to apply (see the end of [1]). However, Theorem 5.1 appears to be limited to proving irreducibility of individual polynomials rather than families of polynomials such as $T^n - 2$ as n varies, which can be treated by the Eisenstein criterion.

6. Going beyond integer coefficients

The rings $\mathbf{Z}$ and $F[X]$ are analogous (*e.g.*, both have division with remainder, leading to similar proofs in both cases that all of their ideals are principal). Therefore $F[X,Y] = F[X][Y] = F[Y][X]$ is analogous to $\mathbf{Z}[X]$. Our two irreducibility tests, regarded as tests for irreducibility in $\mathbf{Z}[T]$ rather than in $\mathbf{Q}[T]$, can be adapted to $F[X,Y]$ by viewing a polynomial in $F[X,Y]$ as a polynomial in one indeterminate whose coefficients are polynomials in the other indeterminate.

(i) (Reduction mod $\pi(Y)$) If $f(X,Y) \in F[X,Y]$ is monic in X and there is an irreducible $\pi(Y) \in F[Y]$ such that $\overline{f}(X,Y) \bmod \pi(Y) \in (F[Y]/\pi F[Y])[X]$ is irreducible, then $f(X,Y)$ is irreducible in $F[X,Y]$.

(ii) (Eisenstein) If $f(X,Y) \in F[X,Y]$ is monic in X and, when written as $X^n + a_{n-1}(Y)X^{n-1} + \cdots + a_1(Y)X + a_0(Y)$ in $F[Y][X]$, there is an irreducible $\pi(Y) \in F[Y]$ such that $\pi(Y) \mid a_i(Y)$ for all i and $\pi(Y)^2 \nmid a_0(Y)$ then $f(X,Y)$ is irreducible in $F[X,Y]$.

The proofs of these irreducibility tests are very similar to the proofs over $\mathbf{Q}$, using $F[Y]$ in place of $\mathbf{Z}$ and depending on a suitable form of Gauss' lemma: a polynomial in $F[Y][X]$ that is monic in X and decomposes in $F(Y)[X]$ into two factors with lower X-degree can be rescaled to such a decomposition in $F[Y][X]$. It is left to the reader to work out the proofs of this version of Gauss lemma and of both irreducibility tests above. Here are examples to illustrate the tests.

Example 6.1. The polynomial $X^n + (Y+5)X + (Y-1)$ in $\mathbf{Q}[X,Y]$ is irreducible because when we reduce it modulo $Y+1$ then in $(\mathbf{Q}[Y]/(Y+1))[X] \cong \mathbf{Q}[X]$ it becomes $X^n + 4X - 2$, which is irreducible over $\mathbf{Q}$ by the classical Eisenstein criterion at 2.

Example 6.2. For all $n \geq 1$, the polynomial $X^n - Y$ is irreducible in $\mathbf{C}[X,Y]$ because it is Eisenstein at Y: as a polynomial in X, its constant term is $-Y$ (divisible by Y just once) and all of its other non-leading coefficients in X are 0 (all divisible by Y).

Example 6.3. For all $n \geq 1$, the polynomial $X^n + Y^n - 1$ is irreducible in $\mathbf{C}[X,Y]$ because it is Eisenstein at $Y-1$: as a polynomial in X, its constant term $Y^n - 1$ is divisible by $Y-1$ exactly once and all of its other non-leading coefficients in X are 0 (all divisible by $Y-1$).

Both the reduction mod p test and the Eisenstein criterion can be generalized to $K[T]$ where K is a finite extension of $\mathbf{Q}$, such as $\mathbf{Q}(i)$ or $\mathbf{Q}(\sqrt[3]{2})$.[1] However, formulating this generalization correctly is beyond the scope of this handout. The main difficulty here is

[1]In fact, historically, the Eisenstein criterion was first introduced by Eisenstein as a test for irreducibility of polynomials in $\mathbf{Q}(i)[T]$, not $\mathbf{Q}[T]$.

describing what the substitute for $\mathbf{Z}$ is in a finite extension of $\mathbf{Q}$; it involves algebraic integers, whose subtleties are explained in a course on algebraic number theory. Also prime numbers in the irreducibility tests have to be replaced by *prime ideals*, and a prime number might not generate a prime ideal in a ring larger than $\mathbf{Z}$.

To illustrate a mistake caused by not properly understanding "primes" in finite extensions of $\mathbf{Q}$, $f(T) = T^2 + 1$ is irreducible in $\mathbf{Q}[T]$ because $f(T+1) = T^2 + 2T + 2$ is Eisenstein at 2, but it would be wrong to say $T^2 + 1$ is irreducible in $\mathbf{Q}(\sqrt{2})[T]$ because $f(T+1)$ is Eisenstein at 2 in $\mathbf{Z}[\sqrt{2}][T]$: the number 2 is not prime in $\mathbf{Z}[\sqrt{2}]$, as $2 = \sqrt{2}\sqrt{2}$.[2] Until you learn some algebraic number theory, be cautious about using either of the two irreducibility tests from $\mathbf{Q}[T]$ directly in $K[T]$ where K is a finite proper extension of $\mathbf{Q}$.

7. Going too far beyond integer coefficients

While the previous section shows that the two irreducibility tests initially introduced for polynomials in $\mathbf{Z}[T]$ have a broader scope, it is important not to push an irreducibility test into a place where it makes no sense. In particular, **DO NOT USE THE EISENSTEIN CRITERION IN $\mathbf{F}_p[T]$**. Although $T^3 - 2T - 2$ is irreducible in $\mathbf{F}_5[T]$ since it is cubic without a root in $\mathbf{F}_5$, it is flat-out wrong to say this polynomial is "Eisenstein at 2 in $\mathbf{F}_5[T]$": the number 2 in $\mathbf{F}_5$ is not prime there: 2 is invertible in $\mathbf{F}_p$. The use of primality for the (valid) Eisenstein criterion in $\mathbf{Z}[T]$ is a subtle interplay between the field $\mathbf{Q}$ and its subring $\mathbf{Z}$ whose ratios fill up $\mathbf{Q}$; the primes are from $\mathbf{Z}$ and Gauss' lemma provides the reason that we can pass from $\mathbf{Q}[T]$ to $\mathbf{Z}[T]$. The field $\mathbf{F}_5$ doesn't have a subring analogous to $\mathbf{Z}$ with primes in it.

Another way to see that saying $T^3 - 2T - 2$ is "Eisenstein at 2 in $\mathbf{F}_5[T]$" is a mistake is that such reasoning should also apply over $\mathbf{F}_3$, and in $\mathbf{F}_3[T]$ the polynomial $T^3 - 2T - 2$ is reducible: $T^3 - 2T - 2 \equiv (T-1)(T^2 + T + 2) \bmod 3$.

Appendix A. Relaxing the monicity condition

In Theorem 2.1 we presented Gauss' lemma for monic polynomials in $\mathbf{Z}[T]$. There is a version of it that does not assume the polynomial is monic. Instead we assume the coefficients have greatest common divisor 1.

Definition A.1. A polynomial $f(T) = a_n T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0$ in $\mathbf{Z}[T]$ is called *primitive* if $\gcd(a_0, a_1, \ldots, a_n) = 1$.

If any coefficient is 1 then the polynomial is primitive. In particular, all monic polynomials in $\mathbf{Z}[T]$ are primitive. An example of a primitive polynomial where no coefficient is 1 is $6T^2 + 10T + 15$: although each pair of coefficients is not relatively prime, taken together the triple $(6, 10, 15)$ has greatest common divisor 1.

Theorem A.2. *If $f(T) \in \mathbf{Z}[T]$ is primitive and $f(T) = g(T)h(T)$ in $\mathbf{Q}[T]$ where $\deg g < \deg f$ and $\deg h < \deg f$ then we can write $f(T) = g_1(T)h_1(T)$ in $\mathbf{Z}[T]$, where $g_1(T)$ and $h_1(T)$ are scalar multiples of $g(T)$ and $h(T)$, respectively; in particular, $\deg g_1(T) = \deg g(T) < \deg f(T)$ and $\deg h_1(T) = \deg h(T) < \deg f(T)$.*

Therefore if a primitive polynomial in $\mathbf{Z}[T]$ can't be written as a product of lower-degree polynomials in $\mathbf{Z}[T]$, it is irreducible in $\mathbf{Q}[T]$.

[2] A valid reason that $T^2 + 1$ is irreducible over $\mathbf{Q}(\sqrt{2})$ is that the polynomial has degree 2 and no root in $\mathbf{Q}(\sqrt{2})$, a subfield of the real numbers.

Proof. We mimic the proof of Theorem 2.1. The reasoning in that proof leading to (2.1) did not rely on $f(T)$ being monic so it carries over. Let's review the argument again: extracting a common denominator in $g(T)$ and $h(T)$ lets us write $g(T) = g_0(T)/d$ and $h(T) = h_0(T)/e$ where $g_0(T)$ and $h_0(T)$ are in $\mathbf{Z}[T]$ and d and e are in $\mathbf{Z}^+$, so

$$def(T) = g_0(T)h_0(T)$$

in $\mathbf{Z}[T]$. Factoring out the greatest common divisor of the coefficients of $g_0(T)$ and of $h_0(T)$ lets us write $g_0(T) = ag_1(T)$ and $h_0(T) = bh_1(T)$, where $a, b \in \mathbf{Z}^+$ and $g_1(T)$ and $h_1(T)$ are *primitive* in $\mathbf{Z}[T]$. Thus we get an analogue of (2.1):

$$def(T) = g_0(T)h_0(T) = abg_1(T)h_1(T). \tag{A.1}$$

where $g_1(T) = (d/a)g(T)$ and $h_1(T) = (e/b)h(T)$. From (A.1) we want to show $de = ab$, so $f(T) = g_1(T)h_1(T)$.

Write $f(T) = a_nT^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0$, so $\gcd(a_0, a_1, \ldots, a_n) = 1$ by hypothesis. In (A.1) the coefficients on the left side are dea_i for $i = 0, \ldots, n$ while the coefficients on the right side are all multiples of ab. Therefore $ab \mid dea_i$ for $0 \leq i \leq n$, so ab is a factor of

$$\gcd(dea_0, dea_1, \ldots, dea_n) = de\gcd(a_0, a_1, \ldots, a_n) = de.$$

Set $c = de/ab$, so $c \in \mathbf{Z}^+$ and (A.1) implies

$$cf(T) = g_1(T)h_1(T), \tag{A.2}$$

which looks just like (2.2). The rest of the proof of Theorem 2.1 after (2.2) can be repeated here to prove $c = 1$, since all it depends on is $g_1(T)$ and $h_1(T)$ being primitive (no prime number divides all the coefficients of $g_1(T)$ or of $h_1(T)$). Details are left to the reader. Thus $f(T) = g_1(T)h_1(T)$ in $\mathbf{Z}[T]$ with $g_1(T)$ a scalar multiple of $g(T)$ and $h_1(T)$ a scalar multiple of $h(T)$. □

Here is the reduction mod p test with an assumption of the polynomial being monic replaced by the weaker assumption that it is primitive.

Theorem A.3. *If $f(T) \in \mathbf{Z}[T]$ is primitive and there is a prime p not dividing the leading coefficient of $f(T)$ such that $\overline{f}(T)$ is irreducible in $(\mathbf{Z}/p\mathbf{Z})[T]$ then $f(T)$ is irreducible in $\mathbf{Q}[T]$.*

Proof. The proof of Theorem 3.1 will carry over with a little more attention to the leading coefficients.

It suffices by Theorem A.2 to prove $f(T)$ is not a product of lower-degree factors in $\mathbf{Z}[T]$ in order to know it is not such a product in $\mathbf{Q}[T]$. Assume $f = gh$ for $g, h \in \mathbf{Z}[T]$ with $\deg g < \deg f$ and $\deg h < \deg f$. Looking at the leading coefficients on both sides of $f = gh$ we have lead $f =$ (lead g)(lead h) in $\mathbf{Z}$, so the leading coefficients of $g(T)$ and $h(T)$ are not divisible by p. Therefore the degrees of f, g and h don't drop after reduction mod p:

$$\begin{aligned} \deg \overline{f} &= \deg f, \\ \deg \overline{g} &= \deg g, \\ \deg \overline{h} &= \deg h. \end{aligned}$$

From $f = gh$ in $\mathbf{Z}[T]$ we have $\overline{f} = \overline{g}\overline{h}$ in $(\mathbf{Z}/p\mathbf{Z})[T]$, and $\overline{f}$ being irreducible implies $\overline{g}$ or $\overline{h}$ has degree 0 and the other has degree equal to that of $\overline{f}$, which means g or h has degree equal to that of f. That is a contradiction, just as in the proof of Theorem 3.1. □

Next we present the Eisenstein criterion without assuming the polynomial is monic. Call

$$f(T) = a_nT^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0 \in \mathbf{Z}[T]$$

an *Eisenstein* polynomial at a prime p if $p \nmid a_n$, $p \mid a_i$ for $i = 0, \ldots, n-1$, and $p^2 \nmid a_0$. The new condition here that we did not need to be explicit about in the monic case is that $p \nmid a_n$. For monic polynomials that condition is automatically satisfied when $a_n = 1$.

Theorem A.4. *If $f(T) \in \mathbf{Z}[T]$ is primitive and Eisenstein at a prime p then $f(T)$ is irreducible in $\mathbf{Q}[T]$.*

Proof. Since $f(T)$ is primitive, it suffices to assume $f = gh$ for $g, h \in \mathbf{Z}[T]$ with $\deg g < \deg f$ and $\deg h < \deg f$ and get a contradiction. From the equation $f = gh$ the leading coefficients of g and h are not divisible by p, so f, g, and h in $\mathbf{Z}[T]$ have the same respective degrees as $\overline{f}$, $\overline{g}$, and $\overline{h}$ in $(\mathbf{Z}/p\mathbf{Z})[T]$.

Reducing both sides of $f = gh$ modulo p, we get $\overline{a}_nT^n = \overline{g}\overline{h}$ in $(\mathbf{Z}/p\mathbf{Z})[T]$. By unique factorization in $(\mathbf{Z}/p\mathbf{Z})[T]$, $\overline{g} = \overline{b}T^r$ and $\overline{h} = \overline{c}T^s$ for some nonzero constants $\overline{b}$ and $\overline{c}$ in $\mathbf{Z}/p\mathbf{Z}$ and nonnegative integers r and s. Then

$$r = \deg \overline{g} = \deg g > 0 \qquad \text{and} \qquad s = \deg \overline{h} = \deg h > 0.$$

Therefore $\overline{g}(T)$ and $\overline{h}(T)$ both have constant term 0, so $\overline{g}(0)$ and $\overline{h}(0)$ vanish in $\mathbf{Z}/p\mathbf{Z}$. Thus $g(0)$ and $h(0)$ are multiples of p (this is the same reasoning as in the proof of Theorem 4.1), so

$$a_0 = f(0) = g(0)h(0) \equiv 0 \bmod p^2,$$

which contradicts the Eisenstein property of $f(T)$. □

All of these results carry over to $F[X, Y]$ as irreducibility tests for polynomials that are primitive in X (meaning the coefficients in $F[Y]$ have constant gcd). Formulations of the results and their proofs are left to the reader. We give one example.

Example A.5. For $n \geq 2$ the polynomial $YX^n + (Y+1)X + Y^2 - 1$ in $\mathbf{C}[X, Y]$ is irreducible because it is primitive as a polynomial in X (the X-coefficients Y, $Y + 1$, and $Y^2 - 1$ are collectively relatively prime in $\mathbf{C}[Y]$) and Eisenstein at $Y + 1$: the leading power of X is not divisible by $Y + 1$, all other coefficients are, and the constant term is divisible by $Y + 1$ but not $(Y + 1)^2$.

References

[1] K. S. Brown, Irreducibility Criteria, http://www.mathpages.com/home/kmath406.htm.

[2] Y-G. Chen, G. Kun, G. Pete, I. Z. Ruzsa, and Á. Timár, "Prime values of reducible polynomials, II," *Acta Arith.*, **104** (2002), 117–127