GALOIS THEORY: LECTURE 8

FEBRUARY 26, 2024

Recall that last class we talked about irreducible polynomials and their similarity to prime numbers. One key difference between irreducible polynomials in $\mathbb{Q}[x]$ and prime numbers is that there are simple tests for the former that allow us to recognize them. How do we tell if a given $f \in \mathbb{Q}[x]$ is irreducible? First note that multiplying by a constant doesn't affect irreducibility, so we might as well clear all the denominators and assume $f \in \mathbb{Z}[x]$.

The goal of today is to introduce six tests for irreducibility. As we go, we'll test them on the following example polynomials:

- $x^3 + x + 1$
- $x^4 + 1$
- $x^4 + 4$

Just by looking at them, can you tell which ones are reducible?

1. Rational Root Test

Before stating this in full generality, we give a special case that's striking and easy to remember:

Version 1.0. If $f \in \mathbb{Z}[x]$ is monic and α is a real root, then α is either an integer or is irrational.

Remark. Right away, this gives an instant proof that $\sqrt{2}$ is irrational. More generally, it instantly follows that $\sqrt[k]{n}$ is always irrational, unless n is a perfect k-th power.

It turns out we can make the above theorem more precise (I've highlighted the only change in blue):

Version 2.0. If $f \in \mathbb{Z}[x]$ is monic and α is a real root, then α is either an integer divisor of $f(0)$ or is irrational.

Example 1. This result implies that the only possible rational roots of $f(x) = x^3 + x + 1$ are ± 1. We can easily confirm that neither of these is a root, however! Since any factorization of f must involve a linear factor, we conclude that f must be irreducible.

Example 2. CAUTION. The same approach as above shows that $x^4 + 1$ and $x^4 + 4$ have no rational roots, but we **cannot conclude that these polynomials are irreducible**. Indeed, it turns out that $x^4 + 4$ is reducible! What the rational root test *does* imply, however, is that if these two polynomials factor, they must factor as a product of two irreducible quadratics.

The versions of the rational root test above restricted our polynomial to be monic. It turns out that with a bit of effort, one can derive a more general version from the previous one:

Version 3.0. If $f \in \mathbb{Z}[x]$, say $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, then any rational root takes on the form $\frac{k}{\ell}$ with $\ell \mid a_n$ and $k \mid a_0$.

2. Reduction to $\mathbb{Z}$

Proposition 1. *If $f \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$ (i.e. there exist $g, h \in \mathbb{Z}[x]$ such that $f = gh$).*

We may as well assume our $f \in \mathbb{Z}[x]$ is primitive, i.e. that the coefficients of f are relatively prime (otherwise, divide through by the greatest common divisor of the coefficients without changing the reducibility). We can formalize this observation:

Summary of a lecture by Leo Goldmakher; typed by Jacob Lehmann Duke from notes by Shaurya Taxali.

Lemma 1. *For all $f \in \mathbb{Q}[x]$, there exists a unique $\alpha_f \in \mathbb{Q}_{>0}$ such that $\alpha_f \cdot f \in \mathbb{Z}[x]$ is primitive.*

Felix proposed a proof of existence: multiply the polynomial by the least common multiple of the denominators to create a polynomial in $\mathbb{Z}[x]$, and then divide by the greatest common divisor of its coefficients. You'll prove uniqueness on this week's problem set.

A more remarkable fact about primitive polynomials, discovered by Gauss, is that primitivity is preserved under multiplication:

Lemma 2. *If $g, h \in \mathbb{Z}[x]$ are primitive, so is gh.*

Armed with these two lemmata, we're ready to prove our proposition.

Proof of Proposition 1. We may assume f is primitive. Since f is reducible over $\mathbb{Q}$, there exist $g, h \in \mathbb{Q}[x]$ with $f = gh$. Our first lemma yields $\alpha_g, \alpha_h \in \mathbb{Q}$ such that $\alpha_g \cdot g$ and $\alpha_h \cdot h$ are primitive. Thus,

$$\alpha_g \alpha_h \cdot f = (\alpha_g \cdot g)(\alpha_h \cdot h).$$

On the other hand, each of the factors on the right hand side are primitive, whence $\alpha_g \alpha_h \cdot f$ is primitive (by our second lemma). But by our first lemma, there's a *unique* rational rescaling of f that makes it primitive, whence $\alpha_g \alpha_h = 1$. We conclude that $f = (\alpha_g \cdot g)(\alpha_h \cdot h)$, and both factors on the right hand side are in $\mathbb{Z}[x]$. □

Remark. Our proof yields more than we claimed: given a factorization of some polynomial over $\mathbb{Q}$, we showed that essentially the same factorization works over $\mathbb{Z}$, once we rescale the original factors by some rational number.

Example 3. Consider $f(x) = x^4 + 1$. From the rational root theorem, we know that if this is reducible, then it must be the product of two quadratics. Now we know more: that we may assume these quadratics have integer coefficients. This is a powerful constraint! Write our hypothetical factorization as

$$x^4 + 1 = (ax^2 + bx + c)(dx^2 + ex + f)$$

where $a, b, c, d, e, f \in \mathbb{Z}$. Clearly $a = d = \pm 1$; without loss of generality we may take $a = 1 = d$. Similarly, $c = f = \pm 1$. Summarizing, we have

$$x^4 + 1 = (x^2 + bx \pm 1)(x^2 + ex \pm 1)$$

Following a suggestion of Felix, comparing the coefficients of x^2 on either side, we deduce $be = \pm 2$, so b and e must have different parity. On the other hand, comparing the coefficients of x yields $b + e = 0$, which is impossible. This contradiction proves that $x^4 + 1$ must be irreducible over $\mathbb{Q}$.

This example demonstrates the power of combining the rational root test with the reduction to $\mathbb{Z}[x]$. Still, it's easy to imagine that this becomes much harder for higher degree polynomials. Fortunately, there are other methods of testing irreducibility.

3. Eisenstein's Criterion

One famous irreducibility criterion (which will turn out to be quite useful for us) is the following result, first published by Schönemann and subsequently rediscovered by Eisenstein:

Proposition 2 (Eisenstein's criterion)**.** *Suppose $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there exists a prime p such that p divides all the coefficients apart from a_n, and $p^2 \nmid a_0$, then f is irreducible over $\mathbb{Q}$.*

Example 4. $x^3 - 3x + 3$ must be irreducible over $\mathbb{Q}$.

Example 5. $x^5 + 6x^4 - 3x^3 + 12x^2 - 9x + 3$ is irreducible over $\mathbb{Q}$.

Example 6. Consider $f(x) = x^4 + 1$ again. At first glance, it's clear that Eisenstein doesn't apply. However, Jonathan observed that $f(x+1)$ is irreducible if and only if $f(x)$ is, and

$$f(x+1) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2.$$

Suddenly, Eisenstein applies! It follows that f is irreducible.

It turns out that it's easier to prove Eisenstein's criterion in the following equivalent form:

Proposition 3 (Eisenstein's criterion, equivalent formulation)**.** *Suppose $f \in \mathbb{Z}[x]$ is a primitive polynomial of the form*

$$f(x) = cx^n + p \cdot g(x),$$

where $\deg(g) < n$ and $g \in \mathbb{Z}[x]$. If $p \nmid g(0)$ then f is irreducible over $\mathbb{Q}$.

Proof. Suppose f is reducible over $\mathbb{Q}$ for some f satisfying the hypotheses in Eisenstein's criterion. Gauss' lemma implies that we can write

$$f = hk$$

for some $h, k \in \mathbb{Z}[x]$. We note that both h and k must be primitive, because if either was not, then f would also not be primitive. We also observe that

$$p \cdot g(0) = f(0) = h(0)k(0)$$

so we can conclude that $p \mid h(0)k(0)$. Since p is prime, we must have $p \mid h(0)$ or $p \mid k(0)$. (Below we shall prove that it must divide both!) Without loss of generality, say $p \mid h(0)$. Then we can write

$$h(x) = x^\ell h_1(x) + p \cdot h_2(x)$$

where $p \nmid h_1(0)$ and $\deg h_2 < \ell$; in other words, h_2 consists of all the contiguous terms of h with coefficients (starting with the constant term) that are divisible by p. Writing h in this manner, we see that

$$cx^n + p \cdot g(x) = f(x) = h(x)k(x) = x^\ell h_1(x)k(x) + p \cdot h_2(x)k(x).$$

Moving multiples of p to one side, we can rewrite the equation as

$$x^\ell \big(cx^{n-\ell} - h_1(x)k(x)\big) = p \cdot \big(h_2(x)k(x) - g(x)\big).$$

In particular, we see that x^ℓ must divide the right hand side, whence

$$cx^{n-\ell} - h_1(x)k(x) = p \cdot (\text{some polynomial in } \mathbb{Z}[x]).$$

Reducing (mod p) yields

$$cx^{n-\ell} \equiv h_1(x)k(x) \pmod{p},$$

whence

$$0 \equiv h_1(0)k(0) \pmod{p}.$$

This implies that p divides either $h_1(0)$ or $k(0)$, but by construction, $p \nmid h_1(0)$. It follows that $p \mid k(0)$. We've thus proved that $p^2 \mid h(0)k(0) = p \cdot g(0)$, from which it follows that $p \mid g(0)$. □

Exercise 1. For the proof to work, we require $\ell < n$. Verify that this holds.

Exercise 2. Where in the proof did we use the primitivity of f?

4. Reduction to $\mathbb{F}_p$

A classic number theory trick for proving the nonexistence of integer solutions to a given equation is to reduce (mod n) for some appropriate n and show there are no solutions. For example, there are no solutions to $x^2 + y^2 = 1599$ with $x, y \in \mathbb{Z}$ because any such solution would satisfy $x^2 + y^2 \equiv 3 \pmod{4}$, which is easily seen to have no solutions. A similar principle allows us to test irreducibility of a polynomial:

Proposition 4. *Given $f \in \mathbb{Z}[x]$ and a prime p, denote by $\overline{f}$ the reduction of f (mod p) (i.e. reduce all the coefficients of f to their equivalent in $\mathbb{F}_p$). If $\overline{f}$ is irreducible over $\mathbb{F}_p$ and $\deg f = \deg \overline{f}$, then f is irreducible over $\mathbb{Q}$.*

Proof. If f is reducible over $\mathbb{Q}$, then it factors as a product of two polynomials in $\mathbb{Z}[x]$, each of degree at least 1. Each factor can be reduced (mod p), and $\overline{f}$ is the product of these factors, hence is reducible over $\mathbb{F}_p$. □

Example 7. Let $f(x) = x^3 + x + 1$. It's easy to verify that over $\mathbb{F}_2$, $\overline{f}(x) = x^3 + x + 1$ has no roots. It follows that $\overline{f}$ is irreducible of $\mathbb{F}_2$, since the factorization of any cubic must involve a linear factor. We conclude that f must be irreducible over $\mathbb{Q}$.

Example 8. CAUTION. Noah pointed out that the condition $\deg f = \deg \overline{f}$ is necessary for Proposition 4 to hold. For example, consider

$$f(x) := 2x^2 + 5x + 2.$$

It's easy to see that f is reducible over $\mathbb{Q}$, since $f(x) = (2x + 1)(x + 2)$. On the other hand, over $\mathbb{F}_2$ we have

$$\overline{f}(x) = x,$$

which is irreducible!

Exercise 3. Where in the proof of Proposition 4 did we require $\deg f = \deg \overline{f}$?

Remark. One natural question is whether the converse of Proposition 4 holds. It does not! For example, it turns out (and this is highly non-obvious!) that $x^4 + 1$ is reducible over $\mathbb{F}_p$ for all p, despite being irreducible over $\mathbb{Q}$.

5. PERRON'S TEST

The previous tests all relied on divisibility properties of the coefficients. By contrast, the test below uses only the *magnitudes* of the coefficients.

Proposition 5 (Perron's test)**.** *Given a monic $f \in \mathbb{Z}[x]$ of degree n such that $f(0) \neq 0$. If the magnitude of the $(n-1)$-st coefficient is larger than the sum of the magnitudes of all the other coefficients, then f is irreducible over $\mathbb{Q}$.*

While harder to remember, it might prevent some confusion by stating the above symbolically. Consider some polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $a_0 \neq 0$. If $|a_{n-1}| > |a_0| + |a_1| + \cdots + |a_{n-2}| + 1$, then f is irreducible over $\mathbb{Q}$.

Here's a closely-related result, also due to Perron; I've highlighted the parts of the statement that differ from the above.

Proposition 6 (Follow up to Perron's test)**.** *Given a monic $f \in \mathbb{Z}[x]$ of degree n such that $f(0) \neq 0$ and $f(\pm 1) \neq 0$. If the magnitude of the $(n-1)$-st coefficient is equal to the sum of the magnitudes of all the other coefficients, then f is irreducible over $\mathbb{Q}$.*

6. SCHUR'S TEST

In 1929, Schur observed that any finite truncation of the Taylor series for e^x was irreducible, and similarly for the Taylor series for $\cos x$ and $\frac{\sin x}{x}$. This inspired him to prove irreducibility of general Taylor-series-like polynomials:

Proposition 7 (Schur's test)**.** *Consider any polynomial of the form $f(x) = 1 + a_1 x + \frac{a_2}{2!}x^2 + \ldots + \frac{a_n}{n!}x^n$, where all the $a_i \in \mathbb{Z}$. If $|a_n| = 1$, then f is irreducible over $\mathbb{Q}$.*