GALOIS THEORY : LECTURE 8

LEO GOLDMAKHER

1. EISENSTEIN'S CRITERION, ROUND TWO

We ended last lecture by discussing the irreducibility of polynomials and several tests that could be used to determine irreducibility, including Eisenstein's criterion. The formulation of the criterion from last lecture can be replaced by the following equivalent formulation.

Theorem 1 (Eisenstein's Criterion)**.** *Suppose $f \in \mathbb{Z}[t]$ is a primitive polynomial which can be written in the form $f(t) = ct^n + pg(t)$ for some prime p and some $g(t) \in \mathbb{Z}[t]$ with $\deg g < n$. If $p \nmid g(0)$ then f is irreducible over $\mathbb{Q}$.*

Wyatt pointed out that we don't have to mention that $p \nmid c$, since we already know that f is primitive. We gave the following example to demonstrate the use of the criterion:

Example 1. Prove that $f := \frac{2}{9}t^5 - 5t^3 + 2t - \frac{1}{3}$ is irreducible over $\mathbb{Q}$.

> We observe that if we factor out $\frac{1}{9}$, we can write $f = \frac{1}{9}(2t^5 - 45t^3 + 18t - 3)$. Applying Eisenstein's criterion with $p = 3$ to the polynomial $9f(t)$ shows that $9f(t)$ is irreducible over $\mathbb{Q}$, whence so is f.

Anya pointed out that the criterion can sometimes apply to nonprimitive polynomials as well, since they can be made into primitive polynomials by factoring out the greatest common divisor of the coefficients.

Proof of Eisenstein's criterion. 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 $h, k \in \mathbb{Z}[t]$. 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

$$h(t) = t^\ell h_1(t) + ph_2(t)$$

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

$$ct^n + pg(t) = f(t) = h(t)k(t) = t^\ell h_1(t)k(t) + ph_2(t)k(t).$$

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

$$t^\ell\big(ct^{n-\ell} - h_1(t)k(t)\big) = p\big(h_2(t)k(t) - g(t)\big).$$

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

$$ct^{n-\ell} - h_1(t)k(t) = p \times (\text{some polynomial in } \mathbb{Z}[t]).$$

Date: February 26, 2018.

Based on notes by J. Wyatt Millstone.

Reducing (mod p) yields

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

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 $p^2 \mid h(0)k(0) = pg(0)$, 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?

As an aside, Eisenstein was a prolific mathematician and produced many results besides his criterion, publishing more than 20 papers in a single year. Despite his mathematical success, he died destitute at the age of 29. E. T. Bell claims that Gauss once remarked, "There have been but three epoch-making mathematicians, Archimedes, Newton, and Eisenstein."

At first sight, Eisenstein's criterion seems to have limited utility, since most polynomials cannot be written in the requisite form. However, with an appropriate change of variables it can be applied to many polynomials. Here's one example.

Example 2. Prove that $f(t) = 1 + t + t^2 + \cdots + t^{16}$ is irreducible over $\mathbb{Q}$.

First, note that $f(t)$ is a geometric series, so we can write

$$f(t) = \frac{t^{17} - 1}{t - 1}.$$

Making the substitution $t \mapsto t + 1$ and applying the Binomial Theorem yields

$$\begin{aligned} f(t+1) &= \frac{(t+1)^{17} - 1}{(t+1) - 1} \\ &= \frac{t^{17} + \binom{17}{1}t^{16} + \cdots + \binom{17}{16}t + \binom{17}{17} - 1}{t} \\ &= t^{16} + \binom{17}{1}t^{15} + \cdots + \binom{17}{16} \end{aligned}$$

Now we can apply Eisenstein's criterion: observe that $17 \mid \binom{17}{n}$ whenever $1 \leq n \leq 16$, and that $\binom{17}{16} = 17$. It follows that $f(t+1)$ is irreducible, and we deduce that $f(t)$ is irreducible.

It turns out that we can replace the exponent 16 in the example above by $p - 1$ for any prime p. Primality is required for irreducibility, however; see Problem Set 5. Polynomials like the one above play an important role in algebraic number theory, and will make an appearance later in the semester when we prove the possibility of a straightedge-and-compass construction of the regular 17-gon.

2. Another Trick for Testing Irreducibility

As a motivating example for our next technique, consider the following puzzle.

Question 1. *What integral values of x and y satisfy $x^2 + y^2 = 1234567$?*

Michael observed that for any solution x, y, we would have

$$x^2 + y^2 \equiv 3 \pmod{4}.$$

This is impossible, however, since it can be directly verified that any square must either be congruent to 0 or 1 (mod 4). Therefore, there can be no integers x and y satisfying the initial equality. Thus, rather than working with the given equality directly, we reduced to a small modulus and then were able to conclude with ease. The next proposition follows the same philosophy.

Proposition 2. *Given $f \in \mathbb{Z}[t]$ and a prime p, denote by $[f]$ the reduction of f (mod p). If $[f]$ is irreducible over $\mathbb{F}_p$ and $\deg f = \deg[f]$, then f is irreducible over $\mathbb{Q}$.*

Example 3. Is $f(x) = x^3 - 4x^2 + 7x - 3$ reducible over $\mathbb{Q}$?

We notice that over $\mathbb{F}_2$, f reduces to

$$[f](x) = x^3 + x + 1.$$

Since $[f]$ is a cubic polynomial, it is reducible if and only if it has a linear factor. We can check and see that neither 0 nor 1 is a root of $[f]$. It follows that $[f]$ is irreducible over $\mathbb{F}_2$, so the proposition implies that f must be irreducible over $\mathbb{Q}$.

Sadly, the converse of the proposition is not true.

Example 4. The polynomial x^4+1 is reducible over $\mathbb{F}_p$ for all primes p, but it is irreducible over $\mathbb{Q}$. (Eli proved the irreducibility part of this claim by making the change of variables $x \mapsto x + 1$ and applying Eisenstein. The reducibility part of the claim, however, is highly non-obvious. We shall prove it later this semester.)

The idea of the proof of the proposition is not too difficult.

Proof (sketch) of Proposition. If f is reducible over $\mathbb{Q}$, then it factors, and each factor can be reduced (mod p). Then $[f]$ is the product of these factors, hence is reducible over $\mathbb{F}_p$. □

Exercise 3. Where in this argument do we require $\deg f = \deg[f]$?

We now apply the proposition to a more complicated example.

Example 5. Prove that $f(x) = x^4 + 2$ is irreducible over $\mathbb{Q}$.

Over $\mathbb{F}_2$ we have $[f](x) = x^4$, which is reducible so the proposition doesn't apply. Over $\mathbb{F}_3$, $[f](x) = x^4 - 1$ is reducible, so again the proposition doesn't apply. Over $\mathbb{F}_5$, however, the situation is more complicated. It is not hard to see that $[f]$ has no roots in $\mathbb{F}_5$. However, it may still be the case that $[f]$ is reducible, since it may be possible to write

$$[f](x) = (x^2 + ax + b)(x^2 + cx + d)$$

for some $a, b, c, d \in \mathbb{F}_5$. (Following a question of Daishiro, we noted that if the two quadratic factors weren't monic we could always factor out the leading coefficients to make them so.) Equating coefficients of the powers of x, this gives us four equations:

$$\begin{aligned} a + c &= 0 \\ d + ac + b &= 0 \\ ad + bc &= 0 \\ bd &= 2 \end{aligned}$$

Solving for b, we find that $b = \pm d$. However, considering the last equation, there is no $b \in \mathbb{F}_5$ such that $b^2 = \pm 2$. It follows that $[f]$ does not have a factorization into quadratics, and so $[f]$ is irreducible over $\mathbb{F}_5$. We conclude by the proposition that f is irreducible over $\mathbb{Q}$.

As Ben pointed out, we could have also applied Eisenstein to f to check for irreducibility. These three example polynomials demonstrate how the proposition can be used effectively to check for irreducibility, but it may not always be the best test – and may sometimes fail completely.

There are many other *ad hoc* tricks that can be used for testing for irreducibility. Here's a beautiful but little-known result due to Schur.

Schur's Lemma (1929)**.** For any $c_i \in \mathbb{Z}$ and any $n \in \mathbb{N}$, the polynomial

$$f(x) = 1 + c_1 x + \frac{c_2}{2!}x^2 + \frac{c_3}{3!}x^3 + \cdots + \frac{c_{n-1}}{(n-1)!}x^{n-1} \pm \frac{1}{n!}x^n$$

is irreducible over $\mathbb{Q}$.

As special cases of Schur's Lemma, we see that any truncation of the Taylor series expansions of the exponential function, cosine function, and $\frac{\sin(x)}{x}$ are all irreducible.

We spent the last few minutes of class reviewing some notation. The symbol $\mathbb{Q}[x]$ represents the ring of polynomials with coefficients in $\mathbb{Q}$ with a single indeterminate x. The symbol $\mathbb{Q}(x)$ is the smallest field containing x. Without knowing any further information, all we can conclude is that

$$\mathbb{Q}(x) = \left\{ \frac{p(x)}{q(x)} : p, q \in \mathbb{Q}[x], q \neq 0 \right\}.$$

Note that if we specify x, the two spaces above may be the same. For example, we have $\mathbb{Q}[i] = \mathbb{Q}(i)$.