Math 250A Lecture 16 Notes

Daniel Raban

October 19, 2017

1 More on Irreducibility Tests

1.1 Eisenstein's criterion

Last lecture, we were applying the Eisenstein criterion to $\frac{x^p-1}{x-1} = x^{p-1} + x^{p-1} + \cdots + x + 1$. We saw that if we set $z = x - 1$, this equaled $z^{p-1} + pz^{p-2} + \cdots + p$.

Why does this work? Let $\zeta = e^{2\pi i/p}$, and look at the ring $\mathbb{Z}[\zeta]$. Then p pactorizes as $(1-\zeta)^{p-1}u$ for some unit u. In an algebraic number theory course, we would say that p is "totally ramified," so Eisenstein's criterion applies. Notice that the polynomial has roots $\zeta, \zeta^2, \ldots, \zeta^{p-1}$, the p-th roots of unity. We also have that $(\zeta^k - 1) = (\zeta - 1)(\zeta^{k-1} + \cdots + 1)$. Conversely, $\zeta - 1$ is divisible by $\zeta^k - 1$, so ζ^k is also a root of 1.

1.2 Rational roots

The only linear factors of $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ are of the form $x - b$ for b dividing a_0. This is because $(cx + b)(\cdots) = x^n + \cdots + a_0$, so $1 = c \times *$ and $a_0 = b \times *$.

Example 1.1. It is not possible to trisect the angle of 120° with just a compass and straightedge.[1] We will show that we cannot construct $2\cos(40°)$. We will not prove this here, but any number that can be constructed cannot satisfy an irreducible polynomial of degree n unless n is a power of 2. We want to show that $2\cos(40°)$ satisfies an irreducible polynomial in $\mathbb{Z}[x]$ of degree 3.

Look at $z = e^{2\pi i/9} = \cos(2\pi/9) + i\sin(2\pi/9)$. This is an angle of 40°. Then $2\cos(40°) = z + z^{-1}$. So we have the polynomial

$$0 = z^9 - 1 = (z^3 - 1)(z^6 + z^3 + 1),$$

which means that $z^6 + z^3 + 1 = 0$. Rewriting this as $z^3 + 1 + z^{-3} = 0$ and letting $c = (z + z^{-1})$ we get

$$c^3 - 3c + 1 = 0.$$

[1] Professor Borcherds gets a lot of emails from people claiming to have proven Fermat's last theorem, Goldbach's conjecture, or that is is possible to trisect any angle.

To show that this is an irreducible polynomial, note that c^3-3c+1 has no linear factors over $\mathbb{Q}$. We just have to check that factors of the constant term 1 are not roots.

If a polynomial of degree ≤ 3 has no linear factors, it is irreducible.[2] So c^3-3c+1 is irreducible.

Example 1.2. The polynomials

$$x^{100}+2, \qquad x^{100}+3$$

are both irreducible. This is in contrast to in general, where polynomials of the form x^n+b can have "unexpected" factorizations. For example,

$$x^{100}+4=(x^{50}+2x^{25}+3)(x^{50}-2x^{25}+2).$$

2 Noetherian Rings and Hilbert's Theorem

2.1 Noetherian rings and Noether's theorem

Definition 2.1. A ring is *Noetherian*[3] if all ideals are finitely generated.

Theorem 2.1. *For a ring R, the following are equivalent:*

1. *R is Noetherian.*
2. *Every nonempty set of ideals has a maximal element.*
3. *Every strictly increasing chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ of ideals is finite.*

Proof. (2) $\iff$ (3): First note that (3) $\implies$ (2) is just Zorn's lemma in disguise. To get (2) $\implies$ (3), observe that if $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$ is infinite, then the set $\{I_1, I_2, I_3, \ldots\}$ has no maximal element.[4]

(1) $\implies$ (3): Suppose that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is a chain of ideals. Put $I=\bigcup_i I_i$. Then I is an ideal. By condition (1), $I=(x_1,\ldots,x_n)$, so all x_i are in some I_m. Then $I_m=I_{m+1}=\cdots$.

(3) $\implies$ (1): Pick an ideal I. We want to show that I is finitely generated. Pick any $x_1 \notin I$. If $I=(x_1)$, we are finished. Otherwise, pick $x_2 \in I$ with $x_2 \neq x_1$ and check if $I=(x_1,x_2)$. If we are still not finished, continue abd we get $(x_1) \subseteq (x_1,x_2) \subseteq (x_1,x_2,x_3) \subseteq \cdots$. The infinite chain must stop by condition (3), so $I=(x_1,\cdots,x_n)$ is finitely generated. □

[2] The same method makes it easy to check polynomials of degree ≤ 3, but, in Professor Borcherd's words "degree ≥ 4 is painful."

[3] Emmy Noether found that a lot of theorems proven about polynomial rings using complicated techniques could be simplified by using this condition.

[4] You may notice that we did not use any properties of rings here. This part of the equivalence is just a general fact about partially ordered sets.

Example 2.1. Let $R = K[x_1, x_2, \dots]$. Then $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$, so R is not Noetherian.

Example 2.2. Let $R = \mathbb{Z}$. We have the infinitely *decreasing* chain of ideals $(2) \supsetneq (4) \supsetneq (8) \supsetneq (16) \supsetneq \cdots$. Rings without decreasing chains of ideals are called *Artinian*. It turns out that all Artinian rings are Noetherian.

Theorem 2.2 (Noether)**.** *If R is Noetherian, so is $R[x]$.*

Proof. Suppose I is an ideal of $R[x]$. Look at the chain of ideals of R given by $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$, where I_k is the set of leading coefficients of polynomials in I of degree ≤ 0.

R is Noetherian, so for some m, $I_m = I_{m+1} = I_{m+2} = \cdots$. Pick the set of polynomials of degree 0 whose leading coefficients generate I_0 (which is finitely generated because R is Noetherian). Do this for polynomials of degree 1, 2, etc. We only need to do this finitely many times because $I_m = I_{m+1} = I_{m+2} = \cdots$. We now leave it as an exercise to show that these finite sets generate I. □

2.2 Hilbert's theorem

Theorem 2.3 (Hilbert)**.** *Any ideal of $K[x_1, \dots, x_n]$ is finitely generated.*

Proof. Use induction on number of variables and then use Noether's theorem. □

The following example shows why this is important.

Example 2.3. Recall that ideals of $K[x]$ are generated by 1 element, but this need not be true for $K[x, y]$. Look at the ideal (x^3, x^2y, xy^2, y^2); this ideal must have at least 4 generators because no element in this set generates more than 1 of these 4 elements. In general, ideals of $K[x_1, \dots, x_n]$ need not be generated by n elements.

Example 2.4. This need not hold for infinitely many variables. $K[x_1, x_2, x_3, \dots]$ has the ideal $(x_1, x_2, x_3, \dots)$, which cannot be generated by a finite number of elements.

Example 2.5. Look at the ideal (x) in $K[x, y]$. Then (x) is a ring (but without an identity element) and is not finitely generated as a ring. For example, a generating set could be $\{x, xy, xy^2, \dots\}$. So we must pay attention to the distinction between being finitely generated as an ideal of a ring and being finitely generated as a ring.

2.3 Rings of invariants and symmetric functions

Suppose a group G acts on a vector space V with basis $\{x_1, \dots, x_n\}$. So for $g \in G$,

$$g \cdot x_1 = g_{1,1}x_1 + g_{1,2}x_2 + \cdots + g_{1,n}x_n$$

G also acts on polynomials in $x_1, \dots, x_n$ by $g \cdot (p + q_{=} g \cdot p + g \cdot q$ and $g \cdot (pq) = (g \cdot p)(g \cdot q)$.

Definition 2.2. The *ring of invariants* is the set of polynomials fixed by G (that is, the polynomials p such that $g \cdot p = p$ for all $g \in G$).

Can we find a finite number of invariants so all invariants are polynomials in them with coefficients in K? Hilbert showed that this is often true, and about 50 years later, Nagata found a counterexample which showed that it is not always true.

Definition 2.3. Let V have basis $\{x_1, \dots, x_n\}$, and let G be the symmetric group on $\{x_1, \dots, x_n\}$. The ring of *symmetric functions* is the ring of invariant polynomials.[5]

Example 2.6. Here are some examples of symmetric functions:

$$x_1 + x_2 + x_3 + \cdots x_n$$

$$x_1 x_2 x_3 \cdots x_n$$

$$x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n$$

$$x_1x_2x_3 + x_1x_2x_4 + \cdots + x_1x_3x_4 + \cdots$$

Look at $(x-x_1)(x-x_2)\cdots(x-x_n) = x^n - (\sum x_i)x^{n-1} + (\sum_{i<j} x_ix_j)x^{n-2} + \cdots \pm \prod x_i$. The coefficients of this polynomial are called the *elementary symmetric functions*.

Theorem 2.4. *Any symmetric function is a polynomial in elementary symmetric functions.*

Proof. We produce an algorithm. The key point is to order the monomials in the right way.[6] We say $x_1^{n_1}x_2^{n_2}\cdots \geq x_1^{m_1}x_2^{m_2}\cdots$ if $(n_1, n_2, \dots) \geq (m_1, m_2, \dots)$ in the lexicographic order.

Suppose we have a symmetric polynomial p. Look at the biggest monomial in it, and kill this monomial by subtracting the polynomial

$$q = (x_1 + x_2 + \cdots)^{n_1-n_2}(x_1x_2 + \cdots)^{n_2-n_3}(x_1x_2x_3 + \cdots)^{n_3-n_4}.$$

Note that all these terms are elementary symmetric functions. So $p-q$ has a smaller largest monomial. Repeating this process, we eventually get to 0 because it is not possible to have an infinite sequence of strictly decreasing monomials (exercise). □

[5] Symmetric functions have a very rich combinatorial theory, showing up in places such as the irreducible characters of the symmetric group and the number of Young tableau of a given shape. If you want to learn more about symmetric functions, you should check out my notes on Math 249, Algebraic Combinatorics!

[6] Ordering the monomials of a polynomial is very important in the study of Gröbner bases.