Polynomials II - Divisibility and Irreducibles

Yan Tao

Febuary 13, 2022

1 Divisibility of Polynomials

Definition 1 *Let p and q be polynomials in the complex numbers $\mathbb{C}$. We say that p* ***is divisble by*** *q over $\mathbb{C}$ if there exists a polynomial r such that $p(z) = q(z)r(z)$.*

Problem 1 *By long division (which we learned how to do last week), answer the following:*

- Is $x^3 - 2x^2 + x - 2$ divisible by $x - 2$ over $\mathbb{C}$?

- Is $x^2 - 4x + 3$ divisible by $x + 1$ over $\mathbb{C}$?

- Is $x^4 + 1$ divisible by $x^2 + i$ over $\mathbb{C}$?

There are some tricks to see divisibility more quickly than by long division, so let's establish a couple useful ones.

Problem 2

- *Show that if p is divisible by the linear (degree 1) polynomial $x - a$ over $\mathbb{C}$ if and only if a is a root of p.*

- *Show that if the coefficients of p add up to 0, then p is divisible by $x - 1$ over $\mathbb{C}$.*

For polynomials over the real numbers, we make a similar (but not quite the same) definition:

Definition 2 *Let p and q be polynomials in the real numbers $\mathbb{R}$. We say that p* ***is divisble by*** *q over $\mathbb{R}$ if there exists a polynomial r such that $p(z) = q(z)r(z)$.*

Divisibility over $\mathbb{C}$ and over $\mathbb{R}$ is similar. Because all real numbers are also complex numbers, if p is divisible by q over $\mathbb{R}$ it is also divisible by q over $\mathbb{C}$. The reverse is not true, however - in Problem 1 we see that x^4+1 is divisible by x^2+i over $\mathbb{C}$. But we cannot say that x^4+1 is divisible by x^2+i over $\mathbb{R}$ - because i is not a real number, x^2+i *doesn't exist* over $\mathbb{R}$.

Problem 3 *Show that the tricks proven in Problem 2 still work if we replace $\mathbb{C}$ with $\mathbb{R}$.*

2 Reducibility and Splitting

Definition 3 *Let p be a* ***non-constant*** *polynomial with coefficients in $\mathbb{C}$ (respectively, $\mathbb{R}$)*

- *p is* ***reducible over*** *$\mathbb{C}$ (respectively, over $\mathbb{R}$) if it is divisible by a polynomial q over $\mathbb{C}$ (respectively, over $\mathbb{R}$), where q is not constant and also has smaller degree than p.*
- *p is* ***irreducible over*** *$\mathbb{C}$ (respectively, over $\mathbb{R}$) if it is not reducible over $\mathbb{C}$ (respectively, over $\mathbb{R}$).*
- *p* ***splits over*** *$\mathbb{C}$ (respectively, over $\mathbb{R}$) if it factors into linear factors over $\mathbb{C}$ (respectively, over $\mathbb{R}$); i.e. if there exist $r_1, ..., r_n$ all in $\mathbb{C}$ (respectively, $\mathbb{R}$) such that $p(x) = (x - r_1)...(x - r_n)$.*

Problem 4 *Show that if p is a polynomial of degree at least 2 which splits over $\mathbb{C}$ (respectively, over $\mathbb{R}$), then p is reducible over $\mathbb{C}$ (respectively, over $\mathbb{R}$).*

It's natural to ask whether the converse is true - does every reducible polynomial split? Let us see one example on the next page.

Problem 5 *Let* $p(x) = x^4 + 3x^2 + 2$.

- *Show that* p *is reducible over* $\mathbb{R}$. *(Hint: To find a factor, it might help to make a substitution.)*

- *Show that* p *does not split over* $\mathbb{R}$. *(Hint: If a polynomial splits, its roots should be very easy to find. But does* p *have real roots?)*

Just like with integers, we can factor polynomials into irreducibles. Therefore, it helps a lot to know what the irreducibles are over $\mathbb{C}$ and over $\mathbb{R}$. The following very famous theorem, which we will not prove this time (maybe in the future!), helps us understand polynomials in complex coefficients.

Theorem 1 *(Fundamental Theorem of Algebra) Every polynomial splits over* $\mathbb{C}$.

Problem 6 *Describe all irreducible polynomials over* $\mathbb{C}$.

Over $\mathbb{R}$, the task is a little harder, but not by much. Since this isn't too important, feel free to skip this page if you want.

Problem 7 *(Challenge) Show that every cubic polynomial is reducible over $\mathbb{R}$. (Hint: Consider the cubic formula from last week. Can you show that one of the three roots is real?)*

Problem 8 *(Challenge) Describe all irreducible polynomials over $\mathbb{R}$. (Hint: For any polynomial in real coefficients, we know that it splits over $\mathbb{C}$. Using the fact that it has real coefficients, group the complex roots in a certain way, then factor the polynomial using that grouping as much as you can.)*

3 Polynomials with Rational Coefficients

As we've just seen, finding the irreducible polynomials in the complex and real numbers is simple and not very interesting. The task is much harder (but much more interesting!) over the rational numbers $\mathbb{Q}$. We define the same things we did before, just replacing the number system with $\mathbb{Q}$. So now, for instance, $x^2 - 2$ is not divisible by $x - \sqrt{2}$ over $\mathbb{Q}$, since $x - \sqrt{2}$ doesn't exist over $\mathbb{Q}$.

Problem 9 *Show that $x^2 - 2$ is irreducible over $\mathbb{Q}$. (Hint: Suppose it were reducible. What would the degrees of the factors have to be, and what does that mean?)*

Problem 10 *Show that $x^3 - 2$ is irreducible over $\mathbb{Q}$. (Hint: This is similar to Problem 9.)*

In general, it is very hard to detect irreducibility. For instance, let us try

Problem 11 *(Challenge) Let $p(x) = x^4 + 6x^2 + 25$.*

- *Find all the roots of p. Are any of them rational?*

- *Show that p is not irreducible. (Hint: Finding a factor is really hard, but we can narrow it down a bit using the answer to the previous part.)*

Fortunately, there are some easier ways for us to show whether or not a polynomial is reducible over $\mathbb{Q}$.

4 Testing for Irreducibility

Note that if a polynomial has rational coefficients, we can multiply everything by the common demoninator, so it suffices to consider polynomials with integer coefficients.

Theorem 2 *(Rational Root Theorem) Suppose that p/q is a root of $a_n x^n + ... + a_0$ where p and q are relatively prime integers. Then p divides a_0 and q divides a_n.*

Problem 12 *Let us prove the Rational Root Theorem.*

- *Suppose that p/q is a root of $a_n x^n + ... a_0$. Plug it in to find an equation in terms of $p, q,$ and $a_0, ..., a_n$.*

- *We want an equation in integers so we can test for divisibility. How do we make everything integers? Write down the new equation.*

- *Factor your equation and use the fact that p and q are relatively prime to finish the proof.*

Problem 13 *Show that $3x^3 - 5x^2 + 5x - 2$ is reducible over $\mathbb{Q}$.*

Problem 14 *Can the Rational Root Theorem show if a polynomial is **irreducible**?*

There is a stronger test available which can show irreducibility.

Theorem 3 *(Eisenstein's Criterion) Suppose that* $q(x) = a_n x^n + ... + a_0$ *is a polynomial, and that there exists a prime number* p *such that:*

- p *divides* $a_0, a_1, ..., a_{n-1}$.
- p *does not divide* a_n.
- p^2 *does not divide* a_0.

Then q *is irreducible over* $\mathbb{Q}$.

We'll come back and prove this later.

Problem 15 *Show that the following polynomials are irreducible over* $\mathbb{Q}$.

- $3x^4 + 15x^2 + 10$

- $x^2 - 2$

- $x^3 - 2$

- $x^7 + 15x^5 - 3x^4 + 6x^3 + 9x^2 - 330x + 420$

Problem 16 *For any positive integer* n*, find an irreducible (over* $\mathbb{Q}$*) polynomial of degree* n.

Eisenstein's criterion can also be used on some polynomials where it doesn't seem useful at first glance.

Problem 17 *Let a be any rational number and $q(x) = a_n x^n + ... + a_0$ be a polynomial with rational coefficients. Show that if $q(x + a)$ (the polynomial obtained by substituting $x + a$ in for x) is irreducible, so is $q(x)$. (Hint: Suppose $q(x)$ were reducible. Find a way to reduce $q(x + a)$.)*

Problem 18 *Show that $x^2 + x + 2$ is irreducible over $\mathbb{Q}$. (Hint: Substitute $x + 3$ for x.)*

Problem 19 *(Challenge) Let p be a prime number. Show that $x^{p-1} + ... + x + 1$ is irreducible over $\mathbb{Q}$. (Hint: Find the right substitution.)*

Problem 20 *(Challenge) Let's prove Eisenstein's Criterion. Fix*

$$q(x) = a_n x^n + ... + a_0$$

satisfying the hypotheses. As with most irreducibility proofs we've seen so far, the best course of action will be contradiction, so let's suppose q is reducible, and write its factors as

$$r(x) = b_l x^l + ... + b_0$$
$$s(x) = c_m x^m + ... + c_0$$

Since these have to multiply to q, we must have $l + m = n$.

- *Since p does not divide a_n, what can we say about b_l and c_m?*

- *Since p divides a_0 but p^2 doesn't, what can we say about b_0 and c_0? If your statement contains an either or, assume one of them without loss of generality.*

- *Write out $a_1, a_2, ...,$ etc. in terms of b's and c's, until you see a pattern. (They will get longer and longer, but there's a nice pattern.)*

- *Using what you've proven about b_0 or c_0, show something about b_1 or c_1. Then show something about b_2 or c_2. Notice a pattern? Complete the proof by showing something about b_l or c_m that contradicts what you found in the first part. (Hint: This is a proof by induction.)*