

# Algebra Handout

Aman Jain | [brainiacmaniac31@gmail.com](mailto:brainiacmaniac31@gmail.com)

April 2020

## Overview

This handout is intended for students and preparing for higher level AMC 10/12 problems and the AIME, as well as any other competitions with similar difficulty levels. The handout assumes some knowledge and experience with many algebra topics and techniques, such as factorizations, solving linear systems of equations and quadratic equations in one variable, and functions/polynomials.

## Some Notes on Notation and Terminology

- $\mathbb{Z}$  is the set of integers.
- $\mathbb{Q}$  is the set of rational numbers.
- $\mathbb{R}$  is the set of real number.
- $\mathbb{C}$  is the set of complex numbers.
- $\sum$  represents a sum, and  $\sum_{i=1}^n f(i)$  is the sum of  $f(i)$  taken over all  $i$  in the range  $1 \leq i \leq n$ .
- $\prod$  represents a product, and  $\prod_{i=1}^n f(i)$  is the product of  $f(i)$  taken over all  $i$  in the range  $1 \leq i \leq n$ .
- $\binom{n}{m}$  is a binomial coefficient ( $n$  choose  $m$ ) which is equal to  $\frac{n!}{m!(n-m)!}$ .
- The variable  $i$  will ONLY be used to represent the imaginary unit,  $\sqrt{-1}$ .
- $\in$  literally translates to “in.” If  $a \in \mathbb{Z}$ , for example, we say that  $a$  is in the set of integers. The opposite of  $\in$  is  $\notin$ .
- We say that a polynomial  $p(x)$  is in a set  $\mathbb{A}$  if and only if all coefficients of  $p(x)$  are in the set  $\mathbb{A}$ . For example, a polynomial in  $\mathbb{Z}$  has integral coefficients.

# 1 Polynomials

## Definition of Polynomial

A polynomial is any expression with variables and coefficients, and contains only the operations of adding, subtracting, and multiplying. One important property of polynomials is that all variables have nonnegative integral exponents. For example, the expressions

$$x^2 - 4x + 3, 2xy - y^3 + 4x, xyz + xy - z, 16x^{16} - 15x^{15} + x$$

are all polynomials, while the expressions

$$\frac{1}{x} - \frac{1}{x+1}, xy^2 - 2z + \sqrt{x}, \sqrt[4]{14x^5 + y}$$

are not. Most of the time, we will be dealing with polynomials in only one variable. All polynomials in one variable are functions.

For now, we will only deal with polynomials of one variable.

## Definition of Degree

We say that the *degree* of a polynomial (notated as  $\deg p$  if  $p(x)$  is the polynomial) is the highest exponent present in the polynomial. For example, the degree of  $2x^7 - 4x^4 + x^3 - \frac{1}{2}x + 12$  is a polynomial of degree 7 because the largest exponent present is a 7.

Consider two polynomials  $f(x)$  and  $g(x)$ , with distinct degrees  $F$  and  $G$  respectively. Then,

- $\deg(f + g) = \max(F, G)$
- $\deg(f \cdot g) = F + G$

The proofs for these two are left as exercises.

## Definition of Root

We say that a *root* of a polynomial  $p(x)$  is some number  $z$ , not necessarily real, such that  $p(z) = 0$ . For example, the polynomial  $q(x) = 2x^2 - 8x + 6$  has the two roots  $x = 1$  and  $x = 3$  because  $q(1) = q(3) = 0$ . Roots are very useful with polynomials, because if we know that the polynomial  $p(x)$  has some root  $c$ , then we can factor  $p(x)$  as  $(x - c)q(x)$  for some polynomial  $q(x)$ .

### The Fundamental Theorem of Algebra

The Fundamental Theorem of Algebra states that every single nonconstant polynomial with complex coefficients has at least one complex root. The proof of this theorem is too complicated for this handout, but is easy to find. Now, this may seem somewhat complicated, but let's try and make this simpler. All this is really saying is that, as long as the polynomial  $p(x)$  isn't just a constant like  $p(x) = 14$ , there always exists some complex number, say  $w$ , such that  $p(w) = 0$ .

This is one of the most important theorems in algebra, and it has many useful corollaries. One important one is that a polynomial of degree  $n$  has *exactly*  $n$  roots, not necessarily distinct (this means roots can be repeated, like in the polynomial  $(x + 3)^3(x - 1)^2$ ). This corollary has a simple proof using induction on the degree of a polynomial and the fact that, if  $r$  is a root of  $p(x)$ , then  $p(x) = (x - r)q(x)$  for some polynomial  $q(x)$ .

We are all familiar with the simplest of polynomials, linear equations and quadratics. However, as the degree of our polynomial increases, finding the polynomial's roots becomes more difficult. Luckily, there are some methods none can use to try and find roots. Before we learn these, however, we will cover polynomial division.

## 1.1 Polynomial Division

In number theory and in general, we say that a number  $a$  divides another number  $b$  if  $a$  is a *factor* of  $b$ . But, what does this really mean? Well, when we're dealing with integers,  $a$  is a factor of  $b$  if there is an integer  $c$  such that  $a \cdot c = b$ . Similarly, with polynomials, we say that  $q(x)$  is a factor of  $p(x)$  if there exists another polynomial  $h(x)$  such that  $p(x) = q(x) \cdot h(x)$ . Just like how in number theory we have quotients and remainders, when we divide a polynomial by another polynomial there are quotients and remainders.

### Quotients and Remainders of Polynomials

Given any two nonzero polynomials  $p(x)$  and  $d(x)$ , there exist unique polynomials  $q(x)$  and  $r(x)$  such that  $p(x) = d(x) \cdot q(x) + r(x)$  and  $\deg r < \deg d$ .

*Proof.* Assume that  $q(x)$  and  $r(x)$  aren't unique, such that

$$f(x) = d(x)q_1(x) + r_1(x) = d(x)q_2(x) + r_2(x)$$

and  $q_1 \neq q_2, r_1 \neq r_2$ . Then, since  $d(x)q_1(x) + r_1(x) = d(x)q_2(x) + r_2(x)$ , we know that

$$\begin{aligned} d(x)q_1(x) - d(x)q_2(x) &= r_2(x) - r_1(x) \\ \implies d(x)(q_1(x) - q_2(x)) &= r_2(x) - r_1(x). \end{aligned}$$

However, in our definition we said that  $\deg d > \deg r$ . Since the LHS is either 0 if  $q_1(x) = q_2(x)$ , or its degree is greater than  $\deg d$ , which in turn is greater than the degree of the RHS. Thus, the only possibility is that  $q_1(x) - q_2(x) = 0$ , which means that the RHS is also equal to 0, so  $q_1(x) = q_2(x)$  and  $r_1(x) = r_2(x)$ , a contradiction to our assumption that  $q(x)$  and  $r(x)$  weren't unique. □

#### Remainder Theorem

As a corollary of the previous result, we will introduce the Remainder Theorem. It states that, for some polynomial  $p(x)$ , the remainder when  $p(x)$  is divided by  $x - c$  is  $p(c)$ . The proof is left as an exercise. *Hints: 1*

We can divide polynomials with long division like we divide normally (which we won't cover here), but there is a useful method of dividing polynomials by linear factors (this will ONLY work for linear factors) called *synthetic division* (which also won't be covered here). Now, let's practice with a few problems.

**1.1.1** Divide each of the following polynomials and find the remainder and quotient.

- Divide  $x^2 + 3x - 1$  by  $x + 2$ .
- Divide  $x^3 - 4x + 5$  by  $x^2 + 7x - 2$ .
- Divide  $x^4 + x^3 - 5x^2 + 23x - 20$  by  $x^2 + 3x - 4$ .
- Divide  $20x^{20} - 19$  by  $x - 1$ . *Hints: 2*

**1.1.2** Find the constant  $c$  such that  $x^5 - 4x^4 - 3x^3 + cx^2 - 52x + 24$  is divisible by  $x^2 + 2x - 3$ .

**1.1.3** (1999 AHSME) Let  $P(x)$  be a polynomial such that when  $P(x)$  is divided by  $x - 19$ , the remainder is 99, and when  $P(x)$  is divided by  $x - 99$ , the remainder is 19. What is the remainder when  $P(x)$  is divided by  $(x - 19)(x - 99)$ ? *Hints: 3, 4*

## 1.2 Roots of Polynomials

We have already defined a root of a polynomial  $p(x)$  to be some number  $z$  such that  $p(z) = 0$ . By the Remainder Theorem, we know that if  $z$  is a root of  $p(x)$ , then  $p(x) = (x - z)q(x)$  for some polynomial  $q(x)$ .

### The Factor Theorem

The Factor Theorem states that, for any polynomial  $p(x)$ ,  $x - c$  is a factor of  $p(x)$  if and only if  $p(c) = 0$ .

*Proof.* Let's write  $p(x) = (x - c)q(x) + r$ , where  $r$  is the remainder (since we are dividing by a linear factor, the remainder is a constant). If  $p(c) = 0$ , then  $0 = p(c) = (c - c)q(c) + r \implies r = 0$  as desired. Otherwise, assume that  $p(x) = (x - c)q(x)$ . We wish to show that  $p(c) = 0$ . However, this is obvious by letting  $x = c$ .  $\square$

This theorem has a very useful corollary. Let  $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , and let  $r_1, r_2, \dots, r_n$  be the  $n$  roots, not necessarily distinct, of  $p(x)$ . Then, by going through every root of  $p(x)$ , we can factor

$$p(x) = a_n(x - r_1)(x - r_2) \dots (x - r_n).$$

This factorization leads us into our next major formula. Back when you first learned about quadratics, maybe you were taught that the sum of the roots of the quadratic  $ax^2 + bx + c$  is  $-\frac{b}{a}$  and the product of the roots is  $\frac{c}{a}$ . This is a small part of a much larger and very important formula.

### Vieta's Formulas

Vieta's formula relate to *symmetric sums* of the roots of a polynomial. Say we have a polynomial  $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , and the  $n$  roots of  $p(x)$  are  $r_1, r_2, \dots, r_n$ . First, we will define the symmetric sums: Let

$$S_1 = r_1 + r_2 + \dots + r_n$$

be the symmetric sum of the roots taken one at a time. Then,

$$S_2 = r_1 r_2 + r_1 r_3 + \dots + r_{n-1} r_n$$

is the symmetric sum of all pairs of roots. Similarly,

$$S_3 = r_1 r_2 r_3 + r_1 r_2 r_4 + \dots + r_{n-2} r_{n-1} r_n$$

is the symmetric sum of all triples of roots, and so on and so forth until

$$S_n = r_1 r_2 \dots r_n.$$

In general, the  $k$ th symmetric sum  $S_k$ , where  $1 \leq k \leq n$ , is the sum of all  $\binom{n}{k}$  products of  $k$  roots. Vieta's Formulas tell us that

$$S_k = (-1)^k \cdot \frac{a_{n-k}}{a_n}.$$

*Proof.* By our corollary from the Factor Theorem, we know that

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = p(x) = a_n (x - r_1)(x - r_2) \cdots (x - r_n).$$

Since the two polynomials are equivalent, they must have the same coefficients. It is easy and straightforward to see that

$$a_k = a_n \cdot (-1)^{n-k} \cdot S_{n=k}$$

and substituting  $j = n - k$ , we have

$$a_{n-j} = a_n \cdot (-1)^j \cdot S_j$$

which rearranges to the desired conclusion. □

Here are some problems:

**1.2.1** For each of the following, answer the question without finding the roots.

- a) What is the sum of the roots of  $2x^3 - 4x^2 + 13x - 7$ ?
- b) What is the product of the roots of  $20x^{20} - 4x^4 + x - 17$ ?
- c) If  $a, b$ , and  $c$  are the roots of  $x^3 - 4x^2 + 5x - 7$ , compute:
  - i)  $a + b + c$ .
  - ii)  $ab + bc + ca$ .
  - iii)  $a^2 + b^2 + c^2$ .
  - iv)  $\frac{1}{a+b} + \frac{1}{b+c} + \frac{1}{c+a}$ . *Hints: 5*

**1.2.2** (2001 AIME I) Find the sum of the roots, real and non-real, of the equation

$$x^{2001} + \left(\frac{1}{2} - x\right)^{2001} = 0,$$

given that there are no multiple roots. *Hints: 6*

**1.2.3** (2017 AMC 12A) For certain real numbers  $a, b$ , and  $c$ , the polynomial

$$g(x) = x^3 + ax^2 + x + 10$$

has three distinct roots, and each root of  $g(x)$  is also a root of the polynomial

$$f(x) = x^4 + x^3 + bx^2 + 100x + c.$$

What is  $f(1)$ ? *Hints: 7*

**1.2.4** (2019 AIME I) For distinct complex numbers  $z_1, z_2, \dots, z_{673}$ , the polynomial

$$(x - z_1)^3(x - z_2)^3 \cdots (x - z_{673})^3$$

can be expressed as  $x^{2019} + 20x^{2018} + 19x^{2017} + g(x)$ , where  $g(x)$  is a polynomial with complex coefficients and with degree at most 2016. The value of

$$\left| \sum_{1 \leq j < k \leq 673} z_j z_k \right|$$

can be expressed in the form  $\frac{m}{n}$ , where  $m$  and  $n$  are relatively prime positive integers. Find  $m + n$ . *Hints: 8, 9*

Sometimes, it isn't enough to simply know about the sums and products of roots. Often, we will need to know more about individual roots, and even solve for them. While cubic and quartic (degrees 3 and 4) formulas exist similar to the quadratic formula, they are exceedingly complicated and absolutely not worth knowing. Luckily, there are a few ways of identifying roots of polynomials.

### The Rational Root Theorem

Let  $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$  be a polynomial with integer coefficients, and assume that  $a_n$  and  $a_0$  are nonzero. Then, if  $p(x)$  has a rational root  $\frac{s}{t}$ ,  $s$  must divide  $a_0$  and  $t$  must divide  $a_n$ .

*Proof.* Since  $\frac{s}{t}$  is a root of  $p(x)$ , we know that

$$p\left(\frac{s}{t}\right) = a_n \left(\frac{s}{t}\right)^n + a_{n-1} \left(\frac{s}{t}\right)^{n-1} + \cdots + a_1 \left(\frac{s}{t}\right) + a_0 = 0.$$

Multiplying both sides by  $t^n$ , we have

$$a_n s^n + a_{n-1} s^{n-1} t + \cdots + a_1 s t^{n-1} + a_0 t^n = 0 \quad (\clubsuit)$$

$$\implies t(a_{n-1} s^{n-1} + a_{n-2} s^{n-2} t + \cdots + a_1 s t^{n-2} + a_0 t^{n-1}) = -a_n s^n.$$

Since the LHS is an integer divisible by  $t$ , the RHS must also be an integer divisible by  $t$ . Since  $\gcd(s, t) = 1$  because  $\frac{s}{t}$  was a fraction in lowest terms, we know that  $t$  divides  $a_n$ . Similarly, if we instead factor  $(\clubsuit)$  as

$$s(a_n s^{n-1} + a_{n-1} s^{n-2} t + \cdots + a_2 s t^{n-2} + a_1 t^{n-1}) = -a_0 t^n,$$

the LHS is an integer divisible by  $s$ , so the RHS must also be. Just as in the previous proof, it follows that  $s$  divides  $a_0$ .  $\square$

Note that this theorem is only useful if our polynomial has any integer roots; many polynomials do not.

One useful corollary of this theorem is that if  $p(x)$  is a *monic* polynomial (a monic polynomial has leading coefficient 1, so the term with the highest degree is of the form  $x^n$  for some integer  $n$ ), then all rational roots of  $p(x)$  are integers. The proof of this is a straightforward application of the Rational Root Theorem.

Sometimes, rational roots aren't enough; many polynomials have irrational roots. Here are some more results about the coefficients and roots of a polynomial.

### Definition of Conjugates

There are a couple types of conjugates. The first one is a *radical conjugate*. Let  $a, b, c$  be rational numbers such that  $\sqrt{c} \notin \mathbb{Q}$ . Then, the radical conjugate of  $a + b\sqrt{c}$  is  $a - b\sqrt{c}$ . There isn't a common notation for this type of conjugate.



The second type of conjugate is the *complex conjugate*. Let  $a$  and  $b$  be real numbers. Then, the complex conjugate of  $a + bi$  is  $a - bi$ , and this is notated as  $\overline{a + bi} = a - bi$ .

Before reading further, try and investigate why these two conjugates are important.

### Irrational Roots of Polynomials in $\mathbb{Q}$ : Radical Conjugate Roots Theorem

Let  $p(x)$  be a polynomial with rational coefficients, and say that  $z = a + b\sqrt{c}$  is an irrational root of  $p(x)$ , where  $a, b, c \in \mathbb{Q}$  and  $\sqrt{c} \notin \mathbb{Q}$ . Then, the radical conjugate  $a - b\sqrt{c}$  must also be a root of  $p(x)$ .

*Proof.* Consider the polynomial  $f(x) = (x - a - b\sqrt{c})(x - a + b\sqrt{c}) = x^2 - 2ax + a^2 - b^2c$ , and note that the two roots of  $f(x)$  are  $a + b\sqrt{c}$  and  $a - b\sqrt{c}$ . By polynomial division, we can write  $p(x) = f(x)q(x) + r(x)$  where  $\deg r < 2$ . We assumed that  $p(x) \in \mathbb{Q}$ , and we can see that  $f(x)$  also has rational coefficients. Therefore,  $q(x), r(x) \in \mathbb{Q}$ . Since  $a + b\sqrt{c}$  is a root of  $f(x)$  and  $p(x)$ , the LHS is equal to 0 and the RHS is equal to  $r(a + b\sqrt{c}) = 0$ . It isn't possible for a linear equation with rational coefficients to have an irrational root unless it is always equal to zero, so we know that  $r(x) = 0$ . Therefore,  $p(x)$  is divisible by  $f(x)$ , and since  $a - b\sqrt{c}$  is a root of  $f(x)$ , it is also a root of  $p(x)$ .  $\square$

### Irrational Roots of Polynomials in $\mathbb{Q}$ : Complex Conjugate Roots Theorem

Let  $p(x)$  be a polynomial with real coefficients, and say that  $w = a + bi$  is an irrational root of  $p(x)$ , where  $a$  and  $b$  are real. Then, the complex conjugate  $\overline{w} = a - bi$  must also be a root of  $p(x)$ .

*Proof.* Consider the polynomial  $f(x) = (x - a - bi)(x - a + bi) = x^2 - 2ax + a^2 + b^2$ , and note that the two roots of  $f(x)$  are  $a + bi$  and  $a - bi$ . By polynomial division, we can write  $p(x) = f(x)q(x) + r(x)$  where  $\deg r < 2$ . We assumed that  $p(x) \in \mathbb{R}$ , and we can see that  $f(x)$  also has real coefficients. Therefore,  $q(x), r(x) \in \mathbb{R}$ . Since  $a + bi$  is a root of  $f(x)$  and  $p(x)$ , the LHS is equal to 0 and the RHS is equal to  $r(a + bi) = 0$ . It isn't possible for a linear equation with real coefficients to have a nonreal root unless it is always equal to zero, so we know that  $r(x) = 0$ . Therefore,  $p(x)$  is divisible by  $f(x)$ , and since  $a - bi$  is a root of  $f(x)$ , it is also a root of  $p(x)$ .  $\square$

Where does this become useful? Well, let's use an example. Say we have a polynomial  $p(x) = x^4 + 6x^3 - 55x^2 - 556x - 1276$ . By the Rational Root Theorem, it has no rational roots. What if I told you that  $2 + 4\sqrt{3}$  and  $-5 + 2i$  were roots of this polynomial? Well, then you'd be able to tell me all four roots of this polynomial! Now, let's do some problems.

**1.2.5** Find the polynomial of lowest degree with roots  $3, 1 + \sqrt{2}$ , and  $-i$ .

**1.2.6** Let the roots of  $12x^3 - 64x^2 + 57x + 70$  be  $a, b, c$  such that  $a < b < c$ . What is

$$2a + 5b + 7c?$$

**1.2.7** (2017 AMC 12A) A set  $S$  is constructed as follows. To begin,  $S = \{0, 10\}$ . Repeatedly, as long as possible, if  $x$  is an integer root of some polynomial

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

for some  $n \geq 1$ , all of whose coefficients  $a_i$  are elements of  $S$ , then  $x$  is put into  $S$ . When no more elements can be added to  $S$ , how many elements does  $S$  have? *Hints: 10*

**1.2.8** (2018 AIME II) A real number  $a$  is chosen randomly and uniformly from the interval  $[-20, 18]$ . The probability that the roots of the polynomial

$$x^4 + 2ax^3 + (2a - 2)x^2 + (-4a + 3)x - 2$$

are all real can be written in the form  $\frac{m}{n}$ , where  $m$  and  $n$  are relatively prime positive integers. Find  $m + n$ . *Hints: 11*

**1.2.9** Prove that any polynomial of odd degree with real coefficients has at least one real root. *Hints: 12*

### 1.3 Equations with Roots of Polynomial

We now have learned many techniques for dealing with polynomials and their roots. Many times, we will need to use these methods to derive relationships between the roots and other aspects of a polynomial. One important result we have already found is Vieta's Formulas, and they will come in handy here.

#### Newton's Sums

Say we have a polynomial  $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$  with roots  $r_1, r_2, \dots, r_n$ . Furthermore, let

$$\begin{aligned} M_1 &= r_1 + r_2 + \cdots + r_n \\ M_2 &= r_1^2 + r_2^2 + \cdots + r_n^2 \\ &\vdots \\ M_k &= r_1^k + r_2^k + \cdots + r_n^k \\ &\vdots \end{aligned}$$

Now, since we have defined  $r_j, 1 \leq j \leq n$  to be the  $n$  roots of  $p(x)$ , we know that

$$a_n r_j^n + a_{n-1} r_j^{n-1} + \cdots + a_1 r_j + a_0 = 0$$

for all  $1 \leq j \leq n$ . Multiplying each of these by  $r_j^{k-n}$  gives us

$$a_n r_j^k + a_{n-1} r_j^{k-1} + \cdots + a_1 r_j^{k-n+1} + a_0 r_j^{k-n} = 0.$$

Summing this over all roots of  $p(x)$  gives us

$$\begin{aligned} &a_n (r_1^k + r_2^k + \cdots + r_n^k) + a_{n-1} (r_1^{k-1} + r_2^{k-1} + \cdots + r_n^{k-1}) + \cdots \\ &\quad + a_1 (r_1^{k-n+1} + r_2^{k-n+1} + \cdots + r_n^{k-n+1}) + a_0 (r_1^{k-n} + r_2^{k-n} + \cdots + r_n^{k-n}) = 0, \end{aligned}$$

which translates to

$$a_n M_k + a_{n-1} M_{k-1} + \cdots + a_1 M_{k-n+1} + a_0 M_{k-n} = 0.$$

This holds for all integers  $k$ ,

## 2 Hints

1. Let  $p(x) = (x - c)q(x) + r(x)$  and substitute  $c$  for  $x$ .
2. Can you think of a multiple of  $x - 1$  that resembles  $20x^{20} - 19$ ? Try adding 1.
3. If we say that the remainder when is  $r(x)$ , what can we say about  $r(x)$ ? Keep the Remainder Theorem in mind.
4. Since  $r(x)$  must be linear, let  $r(x) = ax + b$ , and substitute some useful values to create a system of equations.
5.  $\frac{1}{a+b} + \frac{1}{b+c} + \frac{1}{c+a} = \frac{1}{s-a} + \frac{1}{s-b} + \frac{1}{s-c}$ , where  $s$  is the sum of  $a, b, c$ . Write this as one fraction and factor, factor, factor to get in all in terms of symmetric polynomials and  $s$ .
6. Clearly we want to use Vieta's Formulas, but don't get tricked. What is the degree of the polynomial?
7. Vieta's isn't the way to go here. What can we say if we know that every root of  $g(x)$  is also a root of  $f(x)$ ?
8. We have the first, second, and third coefficients of our original polynomial. Which symmetric sums can we get from here?
9. Use  $z_1 + z_2 + \cdots + z_{673}$  and  $z_1^2 + z_2^2 + \cdots + z_{673}^2$  to solve for  $z_1 z_2 + z_1 z_3 + \cdots + z_{672} z_{673}$ .
10. Rational Root Theorem. We only want integer roots. What are the possible  $a_n$  and  $a_0$ ?
11. We can't hope to calculate the probability that four roots are all real, so let's narrow it down. Can we find any roots?
12. Assume that all roots are nonreal, and contradict this.