4/8/15

HW 5 due Friday.
HW 6 will follow
I'm not here on Mon Apr 20
Exam 3 Fri Apr 24.

Last time we discussed a chain of fields:

$$\mathbb{Q} \subsetneq \mathbb{Q}_{const} \subsetneq \mathbb{Q}_{rad} \subsetneq \mathbb{Q}_{alg} \subsetneq \mathbb{C}$$

$\mathbb{Q} \subsetneq \mathbb{Q}_{const}$: Pythagoreans
$\mathbb{Q}_{const} \subsetneq \mathbb{Q}_{rad}$: Gauss-Wantzel
$\mathbb{Q}_{rad} \subsetneq \mathbb{Q}_{alg}$: Abel-Ruffini
$\mathbb{Q}_{alg} \subsetneq \mathbb{C}$: Liouville

Recall that

$\mathbb{Q}_{rad}$ = numbers formed from 1 using $+, -, \times, \div, \sqrt{}, \sqrt[3]{}, \sqrt[4]{}, \sqrt[5]{}, \ldots$

$\mathbb{Q}_{alg}$ = complex roots of polynomials with coefficients in $\mathbb{Q}$.

Our next topic is to discuss the extension

$$\mathbb{Q}_{rad} \subseteq \mathbb{Q}_{alg}.$$

The problem comes down to the following:

Let $f(x) \in \mathbb{Q}[x]$. We know that the roots of f depend somehow on the coefficients. Can we express the roots in terms of the coefficients using field operations and "radicals" $\sqrt[n]{\ }$?

If so, then we say the polynomial is

"solvable by radicals"

Examples:

- Degree 1.

If $f(x) = ax + b \in \mathbb{Q}[x]$ with $a \neq 0$ then it has a unique root

$$r = -b/a.$$

Thus f is solvable. ///

↓

- Degree 2.

If $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$ with $a \neq 0$ then the roots are

$$r_1, r_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Thus f is solvable. ///

- Degree 3.

Let $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Q}[x]$ with $a \neq 0$. We saw earlier that f is solvable by the following method:

- substitute $x = y - b/3a$.
- then solve the depressed cubic $f(y)$ using Cardano's formula. ///

- Degree 4.

Let $f(x) = ax^4 + bx^3 + cx^2 + dx + e \in \mathbb{Q}[x]$ with $a \neq 0$.

{

Cardano's student Lodovico Ferrari found a formula for the roots in 1540, by reducing the quartic equation to a cubic.

[You do not want to see the formula.]

Thus every degree 4 polynomial is solvable. ///

- Degree 5.

Some quintic equations can be solved by radicals. For example, the equation

$$x^5 - a = 0$$

has solution $x = \sqrt[5]{a}$

[we take the symbol $\sqrt[5]{a}$ to represent all 5 fifth roots of a.]

But after Ferrari, no one was able to find a general formula for the quintic.

Eventually people decided this problem must be impossible and the race was on to find a proof of impossibility.

I'll try to give you a sense of this without going into all the details.

Assume that the degree n polynomial $f(x)$ has roots $r_1, r_2, r_3, \cdots, r_n$. Then by Descartes' Factor Theorem we have

$$f(x) = (x-r_1)(x-r_2)\cdots(x-r_n).$$

[assume the leading coefficient is 1.]

Expanding this out gives

$$f(x) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots + (-1)^n e_n x^0$$

where $e_1 = r_1 + r_2 + r_3 + \cdots + r_n$

$e_2 = r_1 r_2 + r_1 r_3 + \cdots + r_1 r_n + r_2 r_3 + \cdots + r_{n-1} r_n$

$\vdots$

$e_n = r_1 r_2 r_3 \cdots r_n$.

$\wr$

These $e_1, e_2, \cdots, e_n$ are called the elementary symmetric combinations of the roots.

Examples:

- $f(x) = (x-\alpha)(x-\beta)$

$$= x^2 - (\alpha+\beta)x + \alpha\beta$$

so $e_1 = \alpha + \beta$
$e_2 = \alpha \cdot \beta$

- $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$

$$= x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\alpha\gamma+\beta\gamma)x - \alpha\beta\gamma$$

so $e_1 = \alpha + \beta + \gamma$
$e_2 = \alpha\beta + \alpha\gamma + \beta\gamma$
$e_3 = \alpha\beta\gamma$ ///

Thus we have solved for the coefficients in terms of the roots.

roots $\rightsquigarrow$ coefficients

$r_1, r_2, \cdots, r_n \rightsquigarrow -e_1, +e_2, -e_3, \cdots, (-1)^n e_n$.

✓

The real problem is to go backwards:

Given the elementary symmetric combinations $e_1, e_2, \cdots, e_n$, can we combine them in some way to recover the roots $r_1, r_2, \cdots, r_n$?

==

Let's try a small case. Let

$$f(x) = (x - r_1)(x - r_2) = x^2 - e_1 x + e_2$$

where $e_1 = r_1 + r_2$ & $e_2 = r_1 r_2$.

Can we solve for r_1, r_2 in terms of e_1, e_2?

$e_1 = r_1 + r_2 \rightsquigarrow r_1 = ?$

$e_2 = r_1 \cdot r_2 \qquad\quad r_2 = ?$

We will use an idea of Lagrange called the "Lagrange resolvent":

We define new variables

$$s_1 = r_1 + r_2$$
$$s_2 = r_1 - r_2$$

and note that we can solve for r_1, r_2 in terms of s_1, s_2.

$$r_1 = (s_1 + s_2)/2$$
$$r_2 = (s_1 - s_2)/2.$$

Now we will be done if we can solve for s_1, s_2 in terms of e_1, e_2.

$$s_1 = r_1 + r_2 = e_1 \quad \checkmark$$

$$s_2 = r_1 - r_2 = ?$$

Maybe this didn't help. Maybe it's just as hard to solve for s_2 in terms of e_1, e_2 as it is to solve for r_1 and r_2 individually?

4/10/15

HW 5 due now
HW 6 will be posted on Monday
and due on Wed Apr 22
I'm out of town Mon Apr 20 (sorry)
Exam 3 Fri Apr 24.

Today: HW5 Discussion.

The three main properties of the "equals sign" are

- $x = x \quad \forall x$ (reflexive)
- $x = y \Rightarrow y = x \quad \forall x, y$ (symmetric)
- $x = y$ and $y = z \Rightarrow x = z \quad \forall x, y, z$ (transitive)

More generally, we say that any relation $\sim$ satisfying these three properties is an equivalence.

The most famous equivalence after the equals sign is

Equivalence mod n.

Fix a nonzero integer $n \in \mathbb{Z}$ and for all integers $x, y \in \mathbb{Z}$ define

$$x \sim_n y \iff n \mid (x-y).$$

Remark: The symbol $b \mid a$ ("b divides a") means that there exists an integer $k \in \mathbb{Z}$ such that $a = bk$.

So we can rephrase equivalence mod n as

$$x \sim_n y \iff \exists k \in \mathbb{Z},\ x - y = nk.$$

Theorem: $\sim_n$ satisfies the three properties of equivalence.

Proof: Given $x \in \mathbb{Z}$ we have

$$x - x = 0 = n \cdot \boxed{0}$$ ← it exists! ✓

Given $x, y \in \mathbb{Z}$, assume that $x \sim_n y$, i.e., assume there exists $k \in \mathbb{Z}$ such that $x - y = nk$.

$$y - x = n(\exists ?)$$ ← does there exist an integer to go here?

Then we have

$$\begin{aligned} y - x &= -(x-y) \\ &= -nk \\ &= n(-k). \end{aligned}$$

✓

↖ it exists!

Hence $y \sim_n x$.

Given $x, y, z \in \mathbb{Z}$, assume that $x \sim_n y$ and $y \sim_n z$, i.e., assume that there exist $k, l \in \mathbb{Z}$ such that

$$\begin{aligned} x - y &= nk \\ y - z &= nl. \end{aligned}$$

Question: $x - z = n(\exists ?)$

Yes! Adding the equations gives

$$\begin{aligned} x - z &= (x-y) + (y-z) \\ &= nk + nl \\ &= n(k+l). \end{aligned}$$

✓

↖ it exists!

Hence $x \sim_n z$.

///

So what? Equivalence relations are the same thing as partitions. In the case of $\sim_n$ we have

$$\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$$
$$\cup \{1, 1 \pm n, 1 \pm 2n, \dots\}$$
$$\cup \{2, 2 \pm n, 2 \pm 2n, \dots\}$$
$$\vdots$$
$$\cup \{n-1, n-1 \pm n, n-1 \pm 2n, \dots\}$$

The elements in each part are equivalent mod n. Note that the parts are disjoint because of the transitivity of $\sim_n$.

Q: Did we get everything?

Notation: Given $x \in \mathbb{Z}$, define its equivalence class by

$$[x]_n = \{y \in \mathbb{Z} : x \sim_n y\}$$
$$= \text{the set of integers equivalent to } x \text{ mod } n.$$

Claim: $\mathbb{Z} = [0]_n \sqcup [1]_n \sqcup \cdots \sqcup [n-1]_n$.

Proof: we have already seen that these sets are disjoint (I use $\sqcup$ for disjoint union). We still need to show that they cover $\mathbb{Z}$, i.e., given $x \in \mathbb{Z}$ we must show that $x \in [r]_n$ for some $0 \leq r < n$.

Well, since $n \neq 0$ we can use the Division Theorem to write

- $x = qn + r$
- $0 \leq r < n$

Then since $x - r = nq$ we have $x \sim_n r$ and hence $x \in [r]_n$. ///

This is pretty much the first thing you will see in an "abstract" algebra course.

Why do I bring it up now?

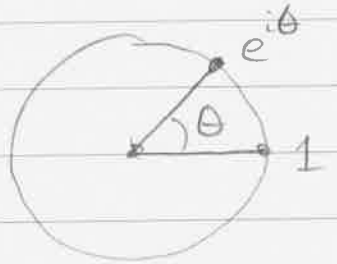
Problem 2. Let $\omega = e^{2\pi i/n}$. Then

$$\omega^k = \omega^l \iff k \sim_n l.$$

This explains the real meaning of equivalence mod n: It tells us when two n^{th} roots of 1 are equal.

Proof: Recall the important fact

$$e^{i\theta} = 1 \iff \theta \in 2\pi\mathbb{Z}$$



Then we have

$$\omega^k = \omega^l \iff \omega^k/\omega^l = 1$$

$$\iff \omega^{k-l} = 1$$

$$\iff e^{2\pi i(k-l)/n} = 1$$

$$\iff 2\pi(k-l)/n \in 2\pi\mathbb{Z}.$$

$\Longleftrightarrow$ $\exists\, m \in \mathbb{Z}$ such that

$$2\pi(k-l)/n = 2\pi m$$

$\Longleftrightarrow$ $\exists\, m \in \mathbb{Z}$ such that

$$k - l = nm$$

$\Longleftrightarrow$ $k \sim_n l$.

This is just a convenient notation so we don't have to write out the details every time.

4/13/15

HW 6 will be posted today
— due next Wed Apr 22
I'm not here on Mon Apr 20
Exam 3 Fri Apr 24.

Math Club Today 6:30pm.

We are discussing the "solvability" of polynomial equations.

Suppose $f(x)$ is a polynomial of degree n with roots $r_1, r_2, \dots, r_n$. Then Descartes' Theorem implies

$$f(x) = (x-r_1)(x-r_2)\cdots(x-r_n).$$

Expanding this gives

$$f(x) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots + (-1)^n e_n x^0.$$

The coefficients can be expressed in terms of the roots as follows:

$$e_1 = r_1 + r_2 + \cdots + r_n = \sum_i r_i$$

$$e_2 = r_1 r_2 + r_1 r_3 + \cdots + r_{n-1} r_n = \sum_{i<j} r_i r_j$$

$$e_3 = r_1 r_2 r_3 + r_1 r_2 r_4 + \cdots + r_{n-2} r_{n-1} r_n = \sum_{i<j<k} r_i r_j r_k$$

$$\vdots$$

$$e_n = r_1 r_2 \cdots r_n .$$

These are called the elementary symmetic functrons of the roots. The formulas were first written down in 1579 by Francois Viète, and are sometimes known as "Viète's Formulas".

Q: What do I mean by "symmetric"?

A: Let $F(x_1, x_2, \cdots, x_n)$ be a function with n inputs. We say that F is a symmetric function if it is invariant under permutations of the inputs.

↓

For example,

$$F(x_1, x_2, x_3, \cdots, x_n) = F(x_2, x_1, x_3, \cdots, x_n),$$

and more generally if $\pi : \{1, 2, \cdots, n\} \to \{1, 2, \cdots, n\}$ is any bijection (called a "permutation" of the set $\{1, 2, \cdots, n\}$) we have

$$F(x_1, x_2, \cdots, x_n) = F(x_{\pi(1)}, x_{\pi(2)}, \cdots, x_{\pi(n)}).$$

Theorem: Let

$$f(x) = (x - r_1)(x - r_2) \cdots (x - r_n)$$

and let $(-1)^{n-i} e_i$ be the coefficient of x^i in the expansion of $f(x)$. Then

$$e_i(r_1, r_2, \cdots, r_n)$$

is a symmetric function of the roots.

Proof: Let $\pi : \{1, 2, \cdots, n\} \to \{1, 2, \cdots, n\}$ be any permutation. Then we have

$$(x-r_1)(x-r_2)\cdots(x-r_n) = (x-r_{\pi(1)})(x-r_{\pi(2)})\cdots(x-r_{\pi(n)}),$$

so the coefficients on both sides are the same. ///

This is the key observation that led to Evariste Galois' revolutionary work on the solvability of equations.

Let's apply it to a toy example: the degree 2 polynomial equation. Let

$$f(x) = (x-r_1)(x-r_2) = x^2 - e_1 x + e_2$$

where $e_1 = r_1 + r_2$, $e_2 = r_1 \cdot r_2$. Our goal is to solve for r_1, r_2 in terms of e_1, e_2.

$$\begin{aligned} e_1 &= r_1 + r_2 \\ e_2 &= r_1 \cdot r_2 \end{aligned} \quad \rightsquigarrow \quad \begin{aligned} r_1 &= ? \\ r_2 &= ? \end{aligned}$$

Can we invert this system?

We will use a trick due to Joseph Lagrange called the "Lagrange resolvent".

↓

We define new variables s_1, s_2 by

$$s_1 = r_1 + r_2$$
$$s_2 = r_1 - r_2$$

It is easy to see that

$$r_1 = (s_1 + s_2)/2$$
$$r_2 = (s_1 - s_2)/2$$

Thus we will be done if we can solve for s_1, s_2 in terms of e_1, e_2.

$s_1 = r_1 + r_2 = e_1$ is easy.

But it is actually not possible to express $s_2 = r_1 - r_2$ as a "single-valued" function of e_1 & e_2.

Why not? Because e_1 & e_2 are symmetric functions of r_1, r_2 but $s_2(r_1, r_2) = r_1 - r_2$ is not!

$$s(r_2, r_1) = r_2 - r_1 = -s(r_1, r_2)$$

What can we do? We have to somehow turn $S_2 = r_1 - r_2$ into a symmetric function. The easiest thing is to square it.

$$S_2^2 = (r_1 - r_2)^2.$$

This is symmetric because

$$S_2^2(r_2, r_1) = (r_2 - r_1)^2 = (r_1 - r_2)^2 = S_2^2(r_1, r_2) \quad \checkmark$$

So, can we express S_2^2 in terms of e_1, e_2?

$$S_2^2 = (r_1 - r_2)^2 = r_1^2 - 2r_1r_2 + r_2^2.$$

Recall: $e_1 = r_1 + r_2$, $e_2 = r_1 r_2$.

$$e_1^2 = (r_1 + r_2)^2 = r_1^2 + 2r_1r_2 + r_2^2$$

so that

$$e_1^2 - 4e_2 = (r_1^2 + 2r_1r_2 + r_2^2) - 4r_1r_2$$
$$= r_1^2 - 2r_1r_2 + r_2^2$$
$$= S_2^2$$

GOOD.

This explains why $S_2 = r_1 - r_2$ is a "two-valued" function of the roots; because

$$S_2 = \sqrt{e_1^2 - 4e_2},$$

and the square root has two values.

Finally we can write down the solution.

$$r_1 = \frac{1}{2}(S_1 + S_2)$$

$$= \frac{1}{2}\left(e_1 + \sqrt{e_1^2 - 4e_2}\right)$$

$$r_2 = \frac{1}{2}(S_1 - S_2)$$

$$= \frac{1}{2}\left(e_1 - \sqrt{e_1^2 - 4e_2}\right).$$

This is the familiar Quadratic Formula, but now we understand it better.

Next we'll take another look at the cubic formula.

4/15/15

HW 6 due next Wed.
I'm gone next Mon
Exam 3 next Fri Apr 24.

Recall: Prior to 1830, "algebra" meant the study of solving polynomial equations. Then along came Évariste Galois (1811–1832). While still a teenager (he died age 20) he did work that laid the seeds of a mathematical revolution, transforming "algebra" from the study of equations to the study of

SYMMETRY.

The transformation was completed around 1930 by, among others, Emmy Noether (1882–1935). After that, "algebra" began to absorb ideas from the other branches of mathematics. Today it is undergoing a new transformation that was initiated by, among others, Alexander Grothendieck (1928–2014). This transformation is far from complete....

In the remaining two lectures, I will discuss ideas of Joseph-Louis Lagrange (1736-1813, born "Giuseppe Lodovico Lagrangia") that led to "Galois Theory".

Recall: If

$$f(x) = (x-r_1)(x-r_2)\cdots(x-r_n) = x^n - e_1 x^{n-1} + e_2 x^{n-2} - \cdots + (-1)^n e_n$$

then the coefficients $e_1, e_2, \cdots, e_n$ are symmetric functions in the roots $r_1, r_2, \cdots, r_n$.

To solve the equation means to express the roots $r_1, r_2, \cdots, r_n$ as algebraic functions of the coefficients $e_1, e_2, \cdots, e_n$. Here "algebraic" means using only the operations

$$+, -, \times, \div, \sqrt{\ }, \sqrt[3]{\ }, \sqrt[4]{\ }, \sqrt[5]{\ }, \cdots$$

Since the $e_1, e_2, \cdots, e_n$ are symmetric in the roots and the individual r_i are very much not symmetric, the process of solving an equation is all about "breaking down" the symmetry in an organized way.

//

Last time we saw Lagrange's solution of the quadratic equation.

Now let's look at the cubic

$$(x-r_1)(x-r_2)(x-r_3) = x^3 - e_1 x^2 + e_2 x - e_3$$

where
$$\left.\begin{aligned} e_1 &= r_1 + r_2 + r_3 \\ e_2 &= r_1 r_2 + r_1 r_3 + r_2 r_3 \\ e_3 &= r_1 r_2 r_3 . \end{aligned}\right\} \Longrightarrow \begin{aligned} r_1 &= ? \\ r_2 &= ? \\ r_3 &= ? \end{aligned}$$

Our goal is to invert this system. Lagrange's idea was to define new variables s_1, s_2, s_3 by

$$\begin{aligned} s_1 &= r_1 + r_2 + r_3 \\ s_2 &= r_1 + \omega r_2 + \omega^2 r_3 \qquad (\omega = e^{2\pi i/3}) \\ s_3 &= r_1 + \omega^2 r_2 + \omega r_3 . \end{aligned}$$

You will show on HW6.3 that this linear system has inverse

$$\begin{aligned} r_1 &= (s_1 + s_2 + s_3)/3 \\ r_2 &= (s_1 + \omega^2 s_2 + \omega s_3)/3 \\ r_3 &= (s_1 + \omega s_2 + \omega^2 s_3)/3 . \end{aligned}$$

Thus we will be done if we can solve for s_1, s_2, s_3 in terms of e_1, e_2, e_3.

First, $s_1 = r_1 + r_2 + r_3 = e_1$. Easy ✓.

But, s_2 and s_3 are not symmetric in r_1, r_2, r_3 so it is impossible to express them as "single-valued functions" of e_1, e_2, e_3 (which are symmetric in r_1, r_2, r_3).

What can we do? We must somehow convert s_2, s_3 into symmetric functions.

The Abel-Ruffini theorem says this is impossible in general, so we should expect that any solution for degree 3 will be sort of tricky / accidental.

Here is the solution: I claim that

$$A := s_2^3 + s_3^3$$
$$B := s_2 \cdot s_3$$

are symmetric in r_1, r_2, r_3.

}

Check:

$$s_2 s_3 = (r_1 + \omega r_2 + \omega^2 r_3)(r_1 + \omega^2 r_2 + \omega r_3)$$

$$= r_1^2 + \omega^2 r_1 r_2 + \omega r_1 r_3$$

$$+ \omega r_2 r_1 + 1 r_2^2 + \omega^2 r_2 r_3$$

$$+ \omega^2 r_3 r_1 + \omega r_3 r_2 + 1 r_3^2$$

$$= r_1^2 + r_2^2 + r_3^2$$

$$+ \underbrace{(\omega + \omega^2)}_{-1} r_1 r_2 + \underbrace{(\omega + \omega^2)}_{-1} r_2 r_3 + \underbrace{(\omega + \omega^2)}_{-1} r_1 r_3$$

$$= r_1^2 + r_2^2 + r_3^2 - r_1 r_2 - r_2 r_3 - r_1 r_3$$

Note that this <u>is</u> symmetric, so we should be able to express it in terms of e_1, e_2, e_3. Can we? Note that

$$e_1^2 = (r_1 + r_2 + r_3)^2$$

$$= r_1^2 + r_2^2 + r_3^2 + 2r_1 r_2 + 2r_2 r_3 + 2r_1 r_3$$

$$= r_1^2 + r_2^2 + r_3^2 + 2e_2.$$

Since $s_2 s_3 = r_1^2 + r_2^2 + r_3^2 - e_2$, we have

$$s_2 s_3 = (e_1^2 - 2e_2) - e_2 = e_1^2 - 3e_2. \quad ///$$

Now the hard part. We have to check that $s_2^3 + s_3^3$ is symmetric and then express it via e_1, e_2, e_3.

For now, I'll just tell you the answer:

$$s_2^3 + s_3^3 = 2e_1^3 - 9e_1e_2 + 27e_3. \quad ///$$

Great. But what we really want are s_2, s_3. How can we find them? Consider

$$(u - s_2^3)(u - s_3^3) = u^2 - (s_2^3 + s_3^3)u + s_2^3 s_3^3$$
$$= u^2 - Au + B^3.$$

The roots are

$$s_2^3, s_3^3 = \frac{1}{2}\left(A + \sqrt{A^2 - 4B^3}\right).$$

This tells us that s_2^3 and s_3^3 are "two-valued" functions of r_1, r_2, r_3, corresponding to the two square roots.

[Remark: we have broken the symmetry by going from one-valued (i.e. symmetric) functions to two-valued functions.]

Finally we get

$$s_2, s_3 = \sqrt[3]{\frac{1}{2}\left(A + \sqrt{A^2 - 4B^3}\right)}.$$

These are now "six-valued functions" of r_1, r_2, r_3. Let's assume that we choose one specific value at each step, giving us specific values of s_1, s_2, s_3.

Then the three roots are

$$r_1 = (s_1 + s_2 + s_3)/3$$

$$r_2 = (s_1 + \omega^2 s_2 + \omega s_3)/3$$

$$r_3 = (s_1 + \omega s_2 + \omega^2 s_3)/3$$

DONE!

4/17/15

NO CLASS MONDAY
HW 6 due next Wed
Exam 3 next Fri.

We are discussing Lagrange's solution of the cubic equation. Let

$$(x-r_1)(x-r_2)(x-r_3) = x^3 - e_1x^2 + e_2x - e_3,$$

so $e_1 = r_1 + r_2 + r_3$
$e_2 = r_1r_2 + r_1r_3 + r_2r_3$
$e_3 = r_1r_2r_3$.

Our goal is to solve (algebraically) for the roots r_1, r_2, r_3 in terms of the coefficients e_1, e_2, e_3.

Lagrange's trick is to define new variables

$$s_1 = r_1 + r_2 + r_3$$
$$s_2 = r_1 + \omega r_2 + \omega^2 r_3$$
$$s_3 = r_1 + \omega^2 r_2 + \omega r_3$$

where $\omega = e^{2\pi i/3}$.

You will show (HW 6.3) that

$$r_1 = (s_1 + s_2 + s_3)/3$$
$$r_2 = (s_1 + \omega^2 s_2 + \omega s_3)/3$$
$$r_3 = (s_1 + \omega s_2 + \omega^2 s_3)/3.$$

Thus we will be done if we can solve for s_1, s_2, s_3 in terms of e_1, e_2, e_3.

$$s_1 = r_1 + r_2 + r_3 = e_1 \quad \checkmark$$

But s_2 and s_3 are <u>not</u> symmetric in r_1, r_2, r_3 (each takes six values when we permute the roots).

Lagrange's next trick is to define

$$A = s_2^3 + s_3^3$$

$$B = s_2 s_3.$$

We showed last time that $s_2 s_3$ <u>is</u> symmetric in r_1, r_2, r_3. In fact,

$$B = s_2 s_3 = \underbrace{e_1^2 - 3e_2}_{\text{obviously symmetric}}$$

Today let's look at $A = s_2^3 + s_3^3$.

You can check that

$$s_2^3 = r_1^3 + 3\omega r_1^2 r_2 + 3\omega^2 r_1^2 r_3 + 3\omega^2 r_1 r_2^2 + 6\omega^3 r_1 r_2 r_3 + 3\omega r_1 r_3^2 + r_2^3 + 3\omega r_2^2 r_3 + 3\omega^2 r_2 r_3^2 + r_3^3$$

Since $s_3^3 = (s_2^3)^*$ we just replace ω by $\omega^* = \omega^{-1} = \omega^2$ to get

$$s_3^3 = r_1^3 + 3\omega^2 r_1^2 r_2 + 3\omega r_1^2 r_3 + 3\omega r_1 r_2^2 + 6 r_1 r_2 r_3 + 3\omega^2 r_1 r_3^2 + r_2^3 + 3\omega^2 r_2^2 r_3 + 3\omega r_2 r_3^2 + r_3^3$$

Then add them and use the fact that $\omega + \omega^2 = -1$ to get

$$\begin{aligned} s_2^3 + s_3^3 = \quad & 2r_1^3 \\ & -3r_1^2 r_2 \quad -3r_1^2 r_3 \\ & -3r_1 r_2^2 + 12 r_1 r_2 r_3 \quad -3r_1 r_3^2 \\ & + 2r_2^3 \quad -3r_2^2 r_3 \quad -3r_2 r_3^2 \quad + 2r_3^3 \end{aligned}$$

Yay, this is symmetric! Now we want to express it in terms of e_1, e_2, e_3.

How? There is an algorithm due to Carl Friedrich Gauss. The important idea is to define the leading term of a polynomial in the 3 variables r_1, r_2, r_3.

Basically, we pick an ordering (say $r_1 > r_2 > r_3$) and then use dictionary order to rank the terms.

In $s_2^3 + s_3^3$ above, the leading term is $2r_1^3 = 2r_1 r_1 r_1$ because it comes first in the dictionary.

$$s_2^3 + s_3^3 = \underline{2r_1^3} + \text{lower terms}$$

Then Gauss says to find a product of e_i's with the same leading term. We have

$$e_1 = r_1 + \text{lower terms}$$
$$e_2 = r_1 r_2 + \text{lower terms}$$
$$e_3 = r_1 r_2 r_3 + \text{lower terms}$$

Hence $2e_1^3 = \underline{2r_1^3} + \text{lower terms}$

Now subtract to get

$$s_2^3 + s_3^3 - 2e_1^3 = \underline{-9r_1^2 r_2} + \text{lower terms.}$$

We need a product of e_i's with leading term $-9r_1^2 r_2$. What is it?

$$-9e_1 e_2 = \underline{-9r_1^2 r_2} + \text{lower terms.}$$

Subtract to get

$$s_2^3 + s_3^3 - 2e_1^3 - (-9e_1 e_2) = \underline{27r_1 r_2 r_3} + 0.$$

Finally subtract $27e_3 = 27r_1 r_2 r_3$

to get

$$s_2^3 + s_3^3 - 2e_1^3 - (-9e_1e_2) - 27e_3 = 0.$$

$$s_2^3 + s_3^3 = 2e_1^3 - 9e_1e_2 + 27e_3 \quad \checkmark$$

Q: Why did the algorithm work?

A: Because at each step the leading term gets smaller in dictionary order. This can't go on forever. ///

The last step is to solve for s_2 and s_3 individually. We did this last time.

$$(u - s_2^3)(u - s_3^3) = u^2 - (s_2^3 + s_3^3)u + s_2^3 s_3^3$$
$$= u^2 - Au + B^3$$

has roots

$$s_2^3, s_3^3 = \frac{1}{2}\left(A + \sqrt{A^2 - 4B^3}\right).$$

Break the symmetry to choose specific values.

Then choose any specific values for the cube roots

$$s_2 = \sqrt[3]{s_2^3} \quad , \quad s_3 = \sqrt[3]{s_3^3} \quad .$$

The values you obtain for s_1, s_2, s_3 are not unique. But it is true that the three roots are given by

$$r_1 = (s_1 + s_2 + s_3)/3$$
$$r_2 = (s_1 + \omega^2 s_2 + \omega s_3)/3$$
$$r_3 = (s_1 + \omega s_2 + \omega^2 s_3)/3 \, .$$

[I choose not to write the full solution in terms of e_1, e_2, e_3. Let's just think of it as an algorithm.] .

///

Example: Consider the polynomial

$$(x-r_1)(x-r_2)(x-r_3) = x^3 - 6x - 6 \, .$$

On HW6.4 you will show that one valid choice of s_i's is

$$s_1 = 0$$
$$s_2 = 3 \cdot \sqrt[3]{2} \approx 3.78$$
$$s_3 = 3 \cdot \sqrt[3]{4} \approx 4.76 .$$

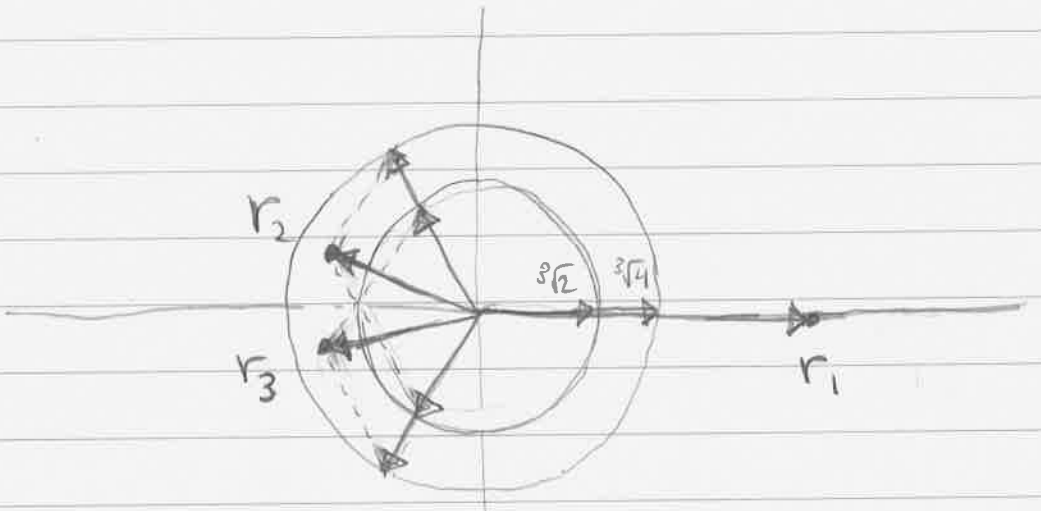
Thus the three roots are given by.

$$r_1 = \sqrt[3]{2} + \sqrt[3]{4}$$

$$r_2 = \omega^2 \cdot \sqrt[3]{2} + \omega \cdot \sqrt[3]{4}$$

$$r_3 = \omega \cdot \sqrt[3]{2} + \omega^2 \cdot \sqrt[3]{4} .$$

Here is a picture:



THE END.