

Activity: Geometric Constructions

Our first application of algebra (to other mathematics) will be to questions of classical geometry. We will look at geometry as it was done in ancient Greece, except that we will use GeoGebra for our constructions.

Our main question is, what can you *construct* using reasonable, fundamental tools. The tools are: an *unmarked straightedge* and a *compass*.

In GeoGebra, there are many more tools than these. Make sure you only use the “new point” tool (to place points at the intersections of lines and circles), the “line through two points” tool, and the “compass” tool (under the circle menu). You can also use the arrow to drag things around if you need to.

To get a feel for the sorts of things you can construct, and maybe things you cannot, here are a few challenges.

1. Can you construct a 60° angle? A 30° angle? If you have constructed any angle at all, can you construct an angle half its measure? That is, can you *bisect* an given angle?
2. Can you construct a square? Can you double the square? That is, if you can construct a square, can you construct a square of twice the area? Careful: this is not a square whose side length is twice the side length of the original.
3. Can you double the circle? That is, can you construct a circle and then construct a second circle of twice the area?
4. Here are three much harder, but related challenges. For each, play around enough to convince yourself these are really hard, if not impossible:
 - (a) Can you *trisect* an angle? That is, given a constructed angle, can you construct an angle $1/3$ its measure?
 - (b) Can you double the *cube*? That is, if you can constructed a cube (or at least a line segment which is the length of the edge of a cube), can you construct cube with twice the volume of the original?
 - (c) Can you square the circle? That is, if you have constructed a circle, can you construct a square that has the same area as the circle?

Activity: Constructible Numbers

We have considered what geometric shapes we could or could not construct. We are left with three big questions: is it possible to *trisect an angle*, to *double a cube*, or to *square a circle*. To answer these questions, we must “algebratize” geometric constructions.

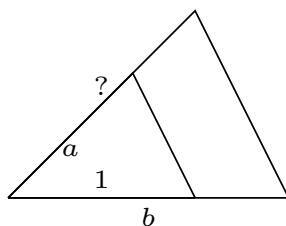
Start with two constructible points 0 and 1 *one unit* apart. We define **constructible** recursively from this base case:

- (a) A **constructible line** is a line passing through two constructible points.
- (b) A **constructible circle** is a circle whose radius is a constructible number and whose center is a constructible point.
- (c) A **constructible point** is the intersection of two constructible lines, two constructible circles, or a constructible line and a constructible circle.

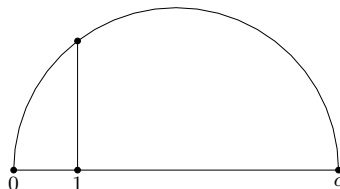
We say a number a is **constructible** provided $a = 0$ or there are two constructible points distance $|a|$ apart. So far we have constructible numbers 0, 1, and -1 . What else is constructible?

For this activity, use GeoGebra. Use only the “new point” tool (to place points at the intersections of lines, circles, or both), the “line through two points” tool, and the “compass” tool (under the circle menu). You can also use the arrow to drag things around if you need to.

1. Show that the numbers 2 and 4 are constructible. Then show that the number $3 = 4 - 1$ is constructible.
2. If a and b are constructible numbers, are the numbers $a + b$ and $a - b$ also constructible?
3. Suppose a and b are constructible. Construct a triangle containing a base of unit length adjacent to a side of length a . Construct a similar triangle with where the side corresponding the unit length side now has length b . What is the length of the side corresponding to the a -length side?



4. Explain how you can modify the above construction to prove that if a and b are constructible, then a/b is constructible.
5. Given constructible number c , explain how you can construct the figure below. The vertical line should be perpendicular to the horizontal line, which is the diameter of the circle.



What is the length of the vertical line?

6. Let \mathfrak{C} be the set of all constructible numbers. What sort of set is this? Is it a group? A ring? A field? Is it one of these we know about already?

6. List five elements in the quotient ring $\mathbb{Q}[x]/\langle p(x) \rangle$ (using the same $p(x)$ from the previous page). Remember, these will all be cosets.

7. The element $x^3 + \langle p(x) \rangle$ is an element of $\mathbb{Q}[x]/\langle p(x) \rangle$, but it can also be written as a “simpler” coset. How?

8. Describe $\mathbb{Q}[x]/\langle p(x) \rangle$ as a set using set builder notation. In other words, this quotient ring is the set of all cosets of the form ...

9. Wait: if we want to show that E is a field, and E is basically the same as $\mathbb{Q}[x]/\langle p(x) \rangle$, then we could just show $\mathbb{Q}[x]/\langle p(x) \rangle$ is a field. What would this mean? What do we need to verify?

Let's explore the connection between extension fields and quotient rings. We have seen that $F[x]/\langle p(x) \rangle \cong F(\alpha)$, where α is a root of its minimal polynomial $p(x)$. The goal of this activity is to see how working in quotient rings help us realize $E = F(\alpha)$ as a field.

We will start easy. For now, let $E = \mathbb{Q}(\sqrt{2})$.

1. What quotient ring is E isomorphic to?
2. One element in E is $1 + 3\sqrt{2}$. What element in the quotient ring does this correspond to?
3. What will $\gcd(3x + 1, x^2 - 2)$ be? How do you know? Then verify you are correct using the Euclidean algorithm.

4. Bezout's identity says that for any polynomials $a(x)$ and $b(x)$, there are polynomials $s(x)$ and $t(x)$ such that

$$\gcd(a(x), b(x)) = s(x)a(x) + t(x)b(x).$$

Find $s(x)$ and $t(x)$ in our case, by working backwards from the Euclidean algorithm above.

5. What does Bezout's identity have to do with the expression

$$1 + \langle x^2 - 2 \rangle = (3x + 1 + \langle x^2 - 2 \rangle)(t(x) + \langle x^2 - 2 \rangle)$$

and what does this have to do with finding inverses? In particular, what is $(1 + 3\sqrt{2})^{-1}$ in E ?

6. Now let's try this again with a more complicated polynomial. As in the earlier activity, take $p(x) = x^3 + 3x^2 - x + 2$ and let ϱ be a root. Use quotient rings to find the inverse of the element $2 + 3\varrho^2$ in $E = \mathbb{Q}(\varrho)$.

Recall that a *basis* for a vector space is a linearly independent spanning set, and that the *dimension* of a vector space is the size of a (any) basis for the space.

If K is an extension field of F , we can view K as a vector space over the field of scalars F . In this case, we say the **degree** of K over F , written $[K : F]$ is the dimension of this vector space.

1. Find a basis for $\mathbb{Q}(\sqrt[3]{5})$ over \mathbb{Q} . What is $[\mathbb{Q}(\sqrt[3]{5}) : \mathbb{Q}]$?
2. Find a basis for $\mathbb{Q}(\sqrt{7})$ over \mathbb{Q} . What is $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}]$?
3. Suppose α is a root of $p(x) = x^5 - 6x^4 + 9x^2 + 3$. Find a basis for $\mathbb{Q}(\alpha)$ over \mathbb{Q} . What is $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.
4. What is the connection between the degree of a field extension and polynomials? Investigate this. In particular, if you claim that you can always find a basis in some systematic way, how do you know it is really a basis? How do you know the basis is linearly independent? How do you know it spans?
5. The polynomial $q(x) = x^7 - 6x^6 - 7x^5 + 51x^4 - 60x^2 - 21$ has α (from question 3) and $\sqrt{7}$ as roots. Does this mean $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$? Why not?

We now have a fairly good idea how to work with $\mathbb{Q}(\alpha)$. What if we consider $\mathbb{Q}(\sqrt[3]{5}, \sqrt{7})$, the smallest field containing \mathbb{Q} , $\sqrt[3]{5}$ and also $\sqrt{7}$?

1. We can think of this as an extension of an extension. Take $\mathbb{Q}(\sqrt[3]{5})$ as our base field. Adjoin to that $\sqrt{7}$ to get $\mathbb{Q}(\sqrt[3]{5}, \sqrt{7})$. What is $[\mathbb{Q}(\sqrt[3]{5}, \sqrt{7}) : \mathbb{Q}(\sqrt[3]{5})]$?
2. What is a basis for $\mathbb{Q}(\sqrt[3]{5}, \sqrt{7})$ over $\mathbb{Q}(\sqrt[3]{5})$? How do you know that this basis spans $\mathbb{Q}(\sqrt[3]{5}, \sqrt{7})$?
3. Using the basis above and the basis for $\mathbb{Q}(\sqrt[3]{5})$ over \mathbb{Q} , find a basis for $\mathbb{Q}(\sqrt[3]{5}, \sqrt{7})$ over \mathbb{Q} .
4. What is $[\mathbb{Q}(\sqrt[3]{5}, \sqrt{7}) : \mathbb{Q}]$? What is the general rule for degrees of extensions of extensions?
5. What is $[\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}) : \mathbb{Q}]$?

We have studied *permutation groups*, as well as groups that do not appear to be groups of permutations (such as \mathbb{Z}_n , $\mathbb{Z}_n \times \mathbb{Z}_m$, groups of functions or matrices, D_4 , etc.). How distinct are these non-permutation groups from permutation groups?

1. Write the 4×4 group tables for \mathbb{Z}_4 and $U(8)$, the group of *units* of \mathbb{Z}_8 (numbers relatively prime to 8) under multiplication.

2. For each element in the groups above, we can see what adding or multiplying it by the other elements does to the other elements. For example, $5 \in U(8)$ corresponds to this function:

$$\lambda_5 = \begin{pmatrix} 1 & 3 & 5 & 7 \\ 5 & 7 & 1 & 3 \end{pmatrix}, \text{ since } 5 \cdot 1 = 5, 5 \cdot 3 = 7, \text{ and so on.}$$

For each element g in each group above, write down the corresponding function λ_g .

3. What happens when you compose two functions λ_g and λ_h for g and h in a group? Try this with a few examples you have above. What do you notice about the function you get?

4. Consider the set $\overline{G} = \{\lambda_g : g \in G\}$. Since each λ_g is a permutation of the elements of G , each of these will be a subset of S_n where $n = |G|$ (in our case, $n = 4$). Is \overline{G} a subgroup of S_4 in both our cases? Will it be a subgroup in general?

Goal: Understand how elements of S_n can be represented as cycles and products of cycles.

1. Can every permutation in S_n be represented using cycle notation? How could you represent the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 2 & 8 & 7 & 9 & 6 & 1 & 4 \end{pmatrix}$?

2. How should we define “cycle”? Write a definition. Some considerations: is $(132)(45)$ a single cycle or two cycles? Is (3124) a cycle? What should we call the **length** of a cycle?

3. Here are a few permutations of S_7 , written as products of cycles. Are there other ways to write each of these using cycle notation? What makes two products of cycles the *same*?

$$(142)(2534)(46)(135) \qquad (12546) \qquad (16)(14)(15)(12) \qquad (12)(37)(25)(37)(45)(46)$$

4. Can the cycle (13254) be written as the product of transpositions? Can it be written as the product of transpositions in more than one way?

- 11

To prove that there is a degree 5 polynomial that is not solvable by radicals, we need to understand how S_5 works. Today we will prove that S_5 is not a *solvable* group.

To do this, we can show that A_5 is simple, because then the only normal series we can get for S_5 will be

$$S_5 \supset A_5 \supset \{(1)\}$$

but A_5 is not abelian, so S_5 is not solvable.

1. Show that A_5 is generated by the set of 3-cycles. You can do this by showing that every pair of transpositions can be written as a product of 3-cycles.
2. Show that if a normal subgroup N of A_5 contains even one 3-cycle, then it is all of A_5 . Remember, normal subgroups are closed under conjugates (here the conjugate would be aba^{-1} where $a \in A_5$ and $b \in N$).
3. Finally, show that every non-trivial normal subgroup of A_n contains a 3-cycle.

Main Question: What is the remainder when you divide a^p by p ?

1. Compute a^p for various values of a and p . What is your conjecture?

Find the remainders when you perform the following divisions. Try different values of a .

2. a^6 divided by 10?
3. a^9 divided by 15?
4. a^{13} divided by 21?
5. a^{2321} divided by 2419?

The *order* of an element g in a group G is the least natural number n such that $g^n = e$, if such a number exists (otherwise we say the order of g is infinite).

1. Find the orders of the elements of S_5 below:

$$\alpha = (12)$$

$$\alpha = (123)$$

$$\alpha = (1234)$$

$$\alpha = (12345)$$

2. Find an element of S_5 that has an order different from those found above.

3. Let α be an element of S_5 . What is α^{120} ?

4. Is there an element in S_5 that has order 120?

5. What is the largest order of any element in S_5 ?

Main Question: What is the remainder when you divide a^p by p ?

1. Compute a^p for various values of a and p . What is your conjecture?

Find the remainders when you perform the following divisions. Try different values of a .

2. a^6 divided by 10?
3. a^9 divided by 15?
4. a^{13} divided by 21?
5. a^{2321} divided by 2419?

Recall that last semester we saw that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. When does this sort of thing happen?

1. Given positive integers m and n , is it always true that $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$? If this is not always true, for which m and n is it true? Try some (many) examples.
2. Consider \mathbb{Z}_{12} . Can we break this down as the direct product of two smaller \mathbb{Z}_p groups? In other words is $\mathbb{Z}_{12} = \mathbb{Z}_m \times \mathbb{Z}_n$ for some values of m and n ?
3. Suppose your absent minded professor claims the answer is “no” and you don’t feel like arguing. Maybe we can do something similar. Find two subgroups of \mathbb{Z}_{12} , call them H and K , such that $H \cap K = \{0\}$ and $HK = \mathbb{Z}_{12}$. In general, $HK = \{h * k : h \in H, k \in K\}$; here it would be better to write $H + K$.

For any n , the group $U(n)$ is the set of all positive integers less than and relatively prime to n , under multiplication modulo n . For example we saw that $U(8) = \{1, 3, 5, 7\}$ is a group under multiplication modulo 8.

Consider the group $U(28)$. The table below gives the twelve elements with their orders:

g	1	3	5	9	11	13	15	17	19	23	25	27
$\text{ord}(g)$	1	6	6	3	6	2	2	6	6	6	3	2

4. Let $G(n)$ be the set of all elements of order n^k for some k (that is, elements with order some power of n). Find $G(2)$ and $G(3)$ for $U(28)$.

5. Are $G(2)$ and $G(3)$ subgroups of $U(28)$?

6. Do $G(2)$ and $G(3)$ have the property that $G(2) \cap G(3) = \{1\}$ and $U(28) = G(2)G(3)$?

7. Is $U(28) \cong G(2) \times G(3)$? Is $U(28) \cong \mathbb{Z}_m \times \mathbb{Z}_n$ for some values of m and n ?

Let's implement the ideas behind RSA cryptography to create a public encryption key that you can use to have your friends send you secure messages.

We will use SAGE to complete this activity. You can use the interactive SAGE cells in the online version of this activity. Or use the online SAGE cell at <https://sagecell.sagemath.org/>. Of course if you have SAGE installed, you can use that.

1. First you will need to select two very large prime numbers. Let's shoot for 20-25 digits. Luckily, SAGE has the command `next_prime()` which will give you the next prime larger than your input. So pick a random input and get two primes. You will want to save these as a constant. For example (but you will need to find a much bigger numbers):

```
p = next_prime(20)
q = next_prime(30)
p, q
```

(23, 31)

2. Now you can compute $n = pq$ and $m = (p - 1)(q - 1)$.

```
n = p*q
m = (p-1)*(q-1)
n, m
```

(713, 660)

Notice that you *could* ask SAGE to find $m = \varphi(n)$ using `euler_phi(n)`, but you should think about why this is a really really really bad idea. If you want, you can try it below, but maybe first with only small values of p and q .

```
euler_phi(n)
```

660

3. Now we need E and D . Recall that we want $\gcd(E, m) = 1$ and $DE \equiv 1 \pmod{m}$. How are you going to find these?

SAGE has the command `gcd(E, m)` that will compute the gcd of the two inputs. You could try factoring m and looking for a reasonably large value of E , or just guess and check until you find a suitable E .

To find D , there is the command `inverse_mod(E, m)` which will run the Euclidean algorithm forwards and backwards on E and m .

```
# repeatedly pick E until gcd(E,m) = 1.
E = 35
gcd(E, m)
```

5

```
D = inverse_mod(E, m)
D
```

You

can now publish the encryption pair (n, E) so your friends can send you messages. You will need to keep D private. But don't lose it! The whole point is that without p and q , you should not be able to find D again, even if you had n and E . Evaluate the cell below to refer to later:

```
print("Your_public_key,_E_=", E, ";_n_=", n)
print("Your_private_key,_D_=", D)
```

If someone has a message x to send you, they would simply need to compute $x^E \pmod{n}$. SAGE can do this with `mod(x^E,n)`, but if x and E are large, this would take a really long time. Luckily, there is a better way: `power_mod(x,E,n)` computes the same thing, but uses the method of repeated squaring to make this much more efficient.

For example:

```
a = mod(12345^35, 713)
b = power_mod(12345,35,713)
a, b
```

(470, 470)

You will need to use this function to decrypt the message y when you take $y^D \pmod{n}$.

4. When you get an encrypted message, you can assign it to the variable `encrypted` and then decrypt it using the `power_mod` function.

```
encrypted = #paste encrypted message here
decrypted = power_mod(encrypted, D, n)
decrypted
```

5. The last piece of the puzzle is what to do with the number you get out of the decryption. You will find some x , but need that to be translated into text you can read.

This depends on the agreed upon method for translating a string of symbols into numbers. For this lab, you can use the following code to decrypt the message:

```
digits = decrypted.digits(base=128)
letters = [chr(ascii) for ascii in digits]
''.join(letters)
```

Here

is why the code above works. First, we need to agree upon how to translate the original message into a number.

Suppose we have a string called `message`. We can create a list of ASCII code values (0 through 127) using `digits = [ord(letter) for letter in message]`. Here `ord()` converts a single letter into its ASCII code, so we do that for each letter in the message.

We must then convert a collection of letters into a single number base 128. SAGE can do this using the `ZZ()` function. So `ZZ(digits,128)`. This will only work if $128^k < n$, where k is the number of digits. So in practice, we would break the longer message into chunks and encrypt each chunk separately.

To undo this coding, you can break down the received message `decrypted` using `digits = decrypted.digits(base=128)`, which makes a list of digits. Then you can create a list of letters using `letters = [chr(ascii) for ascii in digits]`. Finally, put these letters into a string using `''.join(letters)`.

To practice, you can try encoding and decoding messages below. The first set of cells allow you to encrypt and decrypt a very short message. The second pair show a way to break up the message word by word using for loops break up the message into word-long chunks so there is no limit to the length of the message.

```
message = #paste short message here.
digits = [ord(letter) for letter in message]
message_num = ZZ(digits,128)
```

```
encrypted = power_mod(message_num, E, n)
encrypted
```

```
decrypted = power_mod(encrypted, D, n)
digits = decrypted.digits(base=128)
letters = [chr(ascii) for ascii in digits]
''.join(letters)
```

For longer messages:

```
message = #paste message here, enclosed in quotes.
message_array = message.split()
encrypted = []
for word in message_array:
    digits = [ord(letter) for letter in word]
    word_num = ZZ(digits, 128)
    encrypted.append(power_mod(word_num, E, n))
encrypted
```

```
dec_message_array = []
for num in encrypted:
    decrypted = power_mod(num, D, n)
    digits = decrypted.digits(base=128)
    letters = [chr(ascii) for ascii in digits]
    dec_message_array.append(''.join(letters))
' '.join(dec_message_array)
```

Here is an empty sage cell in case you want to experiment with other commands: