**Math 4030-001/Foundations of Algebra/Fall 2017**

**Ruler/Compass at the Foundations: Constructible Numbers**

**Definition 13.1** (a) A complex number $r$ is **algebraic** if $p(r) = 0$ for some $p(x) \in \mathbb{Q}[x]$. Otherwise $r$ is **transcendental**.

(b) Let $\mathbb{A} \subset \mathbb{C}$ be the set of algebraic numbers.

(c) Given $r \in \mathbb{A}$, there is a unique prime polynomial of the form:

$$f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0 \in \mathbb{Q}[x]$$

with $r$ as a root. This is the **minimal** polynomial of $r$.

**Examples.** (a) All rational numbers, $i$, $\sqrt[n]{2}, \cos(\frac{2\pi}{n})$ are algebraic.

(b) $\pi, e$ are transcendental (this isn't easy to prove!).

*Remark.* If $r \in \mathbb{A}$ and $v \in \mathbb{Q}[r]$, then we saw in the previous section that $v \in \mathbb{A}$, since the vectors $1, v, v^2, .... \in \mathbb{Q}[r]$ are linearly dependent.

**Proposition 13.2.** The set of algebraic numbers $\mathbb{A} \subset \mathbb{C}$ is a field.

**Proof.** Let $r \in \mathbb{A}$. Then $-r, 1/r \in \mathbb{Q}[r]$ are also algebraic by the previous remark (or else one can easily find their minimal polynomials). Let $s \in \mathbb{A}$ be another algebraic number. It suffices to show that both $r + s$ and $r \cdot s$ are algebraic numbers to conclude that $\mathbb{A}$ is a field. To do this, we make a tower of number fields.

Let $F = \mathbb{Q}[r]$ and consider $F[x]$, the commutative ring of polynomials with coefficients in $F$. One such polynomial is the minimal polynomial $f(x) \in \mathbb{Q}[x]$ of $s \in \mathbb{A}$. This may not be prime in $F[x]$, but it will have a prime factor $g(x)$ with $g(s) = 0$. We can then create a new field:

$$F[s]$$

with basis $1, s, ..., s^e$ and scalar field $F$. If $w \in F[s]$, then:

$$w = v_0 + v_1 s + v_2 s^2 + ... + v_e s^e$$

and each $v_j = c_{0,j} + c_{1,j}r + \cdots c_{i,j}r^d \in \mathbb{Q}[r]$. Together, we get:

$$w = \sum_{j=1}^{e} \sum_{i=1}^{d} c_{i,j} r^i s^j$$

so the vectors $w_{i,j} = r^i s^j$ span $F[s]$ with **rational** coefficients.

It follows that $w = r + s$ and $u = rs \in F[s]$ are vectors in a field that is also a vector space with a finite basis and scalar field $\mathbb{Q}$. But then as in the remark above, we may conclude that $w$ and $u$ are algebraic numbers since the vectors $1, w, w^2, ...$ and the vectors $1, u, u^2, ...$ are eventually linearly dependent!

**Example.** Let $r = \sqrt{2}$ and $s = \sqrt{3}$. Then:

$$\sqrt{2} + \sqrt{3} \in F[\sqrt{3}] \text{ for } F = \mathbb{Q}[\sqrt{2}]$$

and since $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are a basis for $F[\sqrt{3}]$ as a vector space with rational coefficients, it follows that:

$$1, (r+s), (r+s)^2, (r+s)^3, (r+s)^4 \in F[\sqrt{3}]$$

must be linearly dependent, and indeed:

$$1 - 10(r+s)^2 + (r+s)^4 = 0$$

as we saw in the previous section. Similarly,

$$1, (rs), (rs)^2, (rs)^3, (rs)^4$$

must be linearly dependent, and indeed $6 - (rs)^2 = 0$.

We turn next to the **constructible numbers**. These are all the complex numbers that can be constructed in a finite number of steps with a straightedge and compass and a plane that is blank except for two marked points 0 and 1. A construction is either:

(i) Drawing a line through two marked points, or

(ii) Drawing a circle centered at a marked point with radius equal to the distance between two marked points.

The **intersection** points of the constructed lines and circles are new marked points that can be used for subsequent constructions.

**Getting Started.** There are three choices for the first construction:

(a) The (real axis) line through 0 and 1.

(b) The unit circle centered at 0.

(c) The unit circle centered at 1.

Draw (a)-(c). This generates four new marked points:

$$-1, 2, \frac{1}{2} + \frac{\sqrt{3}}{2}i, \frac{1}{2} - \frac{\sqrt{3}}{2}i$$

that can be used for subsequent constructions.

**Question.** Which numbers can be constructed and which cannot?

**Proposition 13.3.** Every integer can be constructed.

**Proof.** Suppose $n$ can be constructed. Then the intersection points of the unit circle centered at $n$ with the real axis can be constructed. This includes $n+1$. Similarly, if $-n$ is constructed, then $-n-1$ can be constructed. Therefore, by induction, all integers can be constructed. □

**Construction 1.** Constructing a perpendicular line. If points $p, q \in \mathbb{C}$ and the line $L$ through them have been constructed, then the line $L^{\perp}$ perpendicular to $L$ at the point $p$ can be constructed.

**The Construction.** Centering a compass at $p$ with radius $|q-p|$, draw the circle passing through $q = p + (q-p)$ and $r = p - (q-p)$ on the line $L$. Draw two more circles centered at $q$ and $r$ respectively with radius $2|q-p|$. These circles intersect at points $s$ and $t$. The line through $s$ and $t$ is the desired perpendicular line $L^{\perp}$ through $p$. $\square$

**Proposition 13.4.** Every ordered pair of integers can be constructed.

**Proof.** Draw the $y$-axis using Construction 1. Every ordered pair $(0, b),\ b \in \mathbb{Z}$ can be constructed by the argument in Proposition 13.3. Given $(a, 0)$ and $(0, b)$ draw the perpendiculars to the $x$-axis and $y$-axis, respectively, through these points. These are the lines $x = a$ and $y = b$. Their intersection is the point $(a, b)$.

**Corollary 13.5.** Every rational number can be constructed.

**Proof.** Given the rational number $r = \left[\frac{a}{b}\right] \in \mathbb{Q}$, construct the ordered pair $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ using Proposition 13.4 and then construct the line through $(0, 0)$ and $(a, b)$ and mark the intersection of this line with the line $y = 1$, which is also constructed using Proposition 13.4. This is the point $(r, 1)$. Now draw the circle centered at 0 with radius $r = |(r, 1) - (0, 1)|$. The intersection of this circle with the $x$-axis are the rational numbers $r$ and $-r$.

Next, we move on to prove that the set of all complex numbers that can be constructed is a **field**.

**Construction 2.** Translating a constructible vector. If $z$ and $z_0$ are constructible numbers and $v$ is the vector from $z_0$ to $z$, then $v$ may be translated to start at any other constructible number $w$ and used to construct the new complex number $w + v = w + (z - z_0)$.

**The Construction.** First we construct the line through $w$ parallel to the vector $v$. To do this, draw the line $L$ through $z$ and $z_0$. Set the compass at $w$ and draw a circle of radius $|w - z|$. This will meet $L$ at points $z$ and $z'$ (if it only meets at $z$, which is extremely unlikely, then the line through $z$ and $w$ is perpendicular to $L$). Recenter the compass at $z$ and draw the circle of radius $|w - z|$, then do the same thing at $z'$. The two circles will meet at $w$ and another point $w'$. The line $L'$ through $w$ and $w'$ will be perpendicular to $L$. Now use Construction 1 to draw the line $L''$ perpendicular to $L'$ passing through $w$. This is the desired line through $w$ parallel to the vector $v$.

Now center the compass at $w$ and draw the circle with radius $|z-z_0|$. This meets the line $L''$ at two points: $w+v$ and $w-v$. $\square$

**Proposition 13.6.** If complex numbers $w$ and $z$ can be constructed, then the numbers $-z$ and $w+z$ can be constructed.

**Proof.** To construct $-z$, draw the line $L$ through 0 and $z$, center the compass at 0 and draw the circle of radius $|z|$. This meets $L$ at $z$ and also at $-z$. To construct $w+z$, use Construction 2 to translate the vector pointing from 0 to $w$, making it start at $z$. The tip of the translated vector is the complex number $w+z$. $\square$

In order to move to multiplication, we need to use similar triangles.

**Proposition 13.7.** If positive real numbers $r$ and $s$ can be constructed, then $rs$ can be constructed.

**Proof.** Use Construction 1 to draw the vertical lines $x=1, x=r$ through 1 and $r$, respectively. Place the compass at $(1,0)$ and draw the circle with radius $s$ to mark the point $(1,s)$. Draw the line through 0 and $(1,s)$. The intersection of this line with the vertical line $x=r$ is the point $(r,rs)$. The difference between this point and the point $(r,0)$ is $rs$, which can now be marked on the real line. $\square$

**Proposition 13.8.** If a positive real number $r$ can be constructed, then $1/r$ can be constructed.

**Proof.** Draw the vertical lines $x=1$ and $x=r$ as before. Mark the point $(r,1)$ with a unit circle centered at $(r,0)$, and draw the line through 0 and $(r,1)$. The intersection of this line with the vertical line $x=1$ is the point $(1,1/r)$. $\square$

Recall that the product of complex numbers in polar coordinates is:

$$(r;\theta)\cdot(s;\psi)=(rs;\theta+\psi)$$

For this reason, we need the following:

**Construction 3.** Transporting a constructible angle. If $L$ and $L'$ are two constructed lines meeting at $p$ at an angle $\psi$ and if $L''$ is a third line with marked point $q\in L''$, then a fourth line $L'''$ may be constructed that meets $L''$ at $q$ with the same angle $\psi$.

**The Construction.** Draw the unit circle centered at $p$. This meets $L$ and $L'$ at points $z$ and $z'$. The unit circle centered at $q$ similarly meets $L''$ at a point $z''$. The circle centered at $z''$ with radius $|z-z'|$ now meets the unit circle at a point $z'''$, and the line through $z'''$ and $q$ is the desired line. $\square$

*Remark.* Since circles and lines meet at two points, some choices are made in this construction. The reader should perform this construction (and all the others!) to see how these choices are made.

**Corollary 13.9.** If **complex** numbers $z$ and $w$ are constructible, then $zw$ is constructible.

**Proof.** If $z = (r;\theta)$ and $w = (s;\psi)$ (and neither is zero), then the real numbers $r = |z|$ and $s = |w|$ are constructible, and so $rs$ is constructible. Moreover, the angle between the $x$-axis and the line $L'$ through 0 and $w$ be transported by Construction 3 to the origin and the line $L''$ through 0 and $z$. Intersecting the line $L'''$ with the circle centered at 0 with radius $rs$ results in the numbers $zw$ and $-zw$. □

**Corollary 13.10.** If $z$ is constructible, then $1/z$ is constructible.

**Proof.** Exercise.

This completes the proof that the constructible numbers are a field! We next study this field, with an eye toward understanding which numbers are constructible and which are not.

**Proposition 13.11.** If $r > 0$ is constructible, then $\sqrt{r}$ is constructible.

**Proof.** First of all, notice that $\sqrt{r^2+1}$ may be constructed as the length of the segment between 0 and the constructible point $(r, 1)$. Now intersect the circle with radius $r + 1$ with the line $x = \sqrt{r^2+1}$ and draw the line through this point and the origin. This results in a right triangle with hypotenuse $r + 1$ and horizontal side length $\sqrt{r^2+1}$. By the Pythagorean theorem, the vertical side length $s$ is given by:

$$(r^2 + 1) + s^2 = (r + 1)^2; \text{ so } s = \sqrt{2r}$$

But $\sqrt{2}$ is constructible, so it can be inverted (Proposition 13.8.) and multiplied by $s$ (Proposition 13.7.) to construct the real number $\sqrt{r}$. □

Once again, there is a partner angle construction.

**Construction 4.** Bisecting a constructible angle.

**Proof.** If constructible lines $L$ and $L'$ meet in a (marked) point $p$, draw the unit circle centered at $p$ and mark the intersection points $q$ (with $L$) and $q'$ (with $L'$). Now draw the circles centered at $q$ and at $q'$ with radius $|q - q'|$. These will intersect in two points, and the line through these two points bisects the angle between $L$ and $L'$. □

**Corollary 13.12.** If $z$ is constructible, then $\pm\sqrt{z}$ are constructible.

**Proof.** If $z = (r; \theta)$, take the square root of $r$ (Proposition 13.11) and bisect the angle $\theta$ using Construction 4 to obtain $\sqrt{z} = (\sqrt{r}; \frac{\theta}{2})$.

**Example.** Since $i$ is constructible by Proposition 13.2, we may repeat Corollary 13.2 to construct an infinite sequence of complex numbers:

$$\sqrt{i} = \cos\left(\frac{\pi}{4}\right) + \sin\left(\frac{\pi}{4}\right) i, \sqrt[4]{i} = \cos\left(\frac{\pi}{8}\right) + \sin\left(\frac{\pi}{8}\right) i, ...., \sqrt[2^n]{i}, ...$$

Next, we think about **towers of fields** associated to constructions.

**The Floors of the Tower.** Let $z_1 = (a_1, b_1), ..., z_n = (a_n, b_n)$ be a set of points in the plane and $F \subset \mathbb{R}$ be a field that contains all the coordinates $a_1, ..., a_n, b_1, ..., b_n$ of the points. Let $L, L'$ be lines through pairs of the points and let $C, C'$ be circles centered at one of the points with radius equal to the distance between two of the points. That is, $L, L', C, C'$ are the lines and circles that may be constructed. Then:

(a) The coordinates of the intersection point of $L$ and $L'$ are in $F$.

(b) The coordinates of the intersection points of $L$ and $C$ are in

$$F[\sqrt{\Delta}] \text{ for some } \Delta \in F$$

(c) The coordinates of the intersection points of $C$ and $C'$ are in

$$F[\sqrt{\Delta'}] \text{ for some } \Delta' \in F$$

For (a), the line through $(a_i, b_i)$ and $(a_j, b_j)$ has equation:

$$x(b_i - b_j) - y(a_i - a_j) = b_i a_j - a_i b_j$$

This is an equation of the form $Ax + By = C$ all of whose constants $A, B, C$ are in the field $F$. It follows by row reduction that the common solution to two such equations is $(x, y) = (a, b)$ with $a, b \in F$.

The equation of the circle of radius $|z_j - z_i| = \sqrt{(a_j - a_i)^2 + (b_j - b_i)^2}$ centered at the point $(a_k, b_k)$ is:

$$(x - a_k)^2 + (y - b_k)^2 = (a_j - a_i)^2 + (b_j - b_i)^2$$

This is an equation of the form $(x-a)^2+(y-b)^2 = D$ with $a, b, D \in F$. We may substitute $y = (C - Ax)/B$ into this equation to get:

$$(x - a)^2 + ((C - Ax)/B - b)^2 = D$$

which is a quadratic polynomial in $x$, with solution of the form:

$$x = \frac{-c \pm d\sqrt{\Delta}}{2e}$$

with $c, d, e, \Delta \in F$. In other words, $x \in F[\sqrt{\Delta}]$ (and then $y$ is, too).

Since the constants in the equation of a second circle:

$$(x-a')^2+(y-b')^2=D'$$

are also in $F$, we may subtract the two equations to get:

$$(2a'-2a)x+(a^2-a'^2)+(2b_l-2b_k)y+(b^2-b'^2)=D-D'$$

This is the equation for the line through the intersection points of the two circles, and by the argument of the previous paragraph it intersects either of the circles in a point $(x,y)$ with coordinates in $F[\sqrt{\Delta'}]$.

**Example.** The intersection of the two circles:

$$x^2+y^2=3 \text{ and } (x-1)^2+(y-2)^2=7$$

is computed as follows:

$$\begin{aligned} 7 &= (x-1)^2+(y-2)^2 \\ &= x^2-2x+1+y^2-4y+4 \\ &= (x^2+y^2)+5-2x-4y \\ &= 8-2x-4y \end{aligned}$$

This gives the equation of a line:

$$2x+4y=1$$

with which we continue:

$$\begin{aligned} 3 &= x^2+y^2 \\ &= x^2+((1-2x)/4)^2 \\ &= \tfrac{5}{4}x^2-\tfrac{1}{4}x+\tfrac{1}{16} \end{aligned}$$

to get a quadratic polynomial:

$$20x^2-4x-47=0$$

whose roots are the $x$-coordinates of the intersection of the circles.

$$x=\frac{4\pm\sqrt{3776}}{40}=\frac{1\pm 2\sqrt{59}}{10}$$

Solving the linear equation for $y$, we get

$$y=\frac{2\mp\sqrt{59}}{10}$$

Thus in this example, $\Delta'=59$.

**The Tower.** Start with the field $F=\mathbb{Q}$ of rational numbers. By the result above on the floors of the tower, including the coordinates of each newly constructed complex number either fails to enlarge the field $F$ or else enlarges it to $F[\Delta]$ for some $\Delta\in F$. In the latter case, $F[\Delta]$ is a new field with basis $1,\sqrt{\Delta}$ as a vector space over $F$.

Now suppose $(a, b)$ are the coordinates of a constructible number. Then $v = a$ (and $b$) belong to a field obtained from $\mathbb{Q}$ by a finite number of constructions, enlarging it each time by a square root:

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{\Delta_1}] \subset \mathbb{Q}[\sqrt{\Delta_1}][\sqrt{\Delta_2}] \ \subset ... \subset F$$

Then we have the following:

(i) The dimension of $F$ is $2^n$, as a vector space with rational scalars.

A basis for this space is given by the vectors:

$$\prod_{i=1}^{n} (\sqrt{\Delta_i})^{\epsilon_i} \text{ for } \epsilon_i \in \{0, 1\}$$

(ii) Each $v \in F$ is algebraic, with minimal and characteristic polys:

$$p(x)^m = f(x)$$

(and the characteristic polynomial necessarily has degree $2^n$).

From this we get the following Theorem on constructible numbers.

**Theorem 13.13.** (a) Every constructible number is algebraic.

(b) If $r \in \mathbb{R}$ is constructible and $p(x)$ is its minimal polynomial, then

$$\textit{the degree of } p(x) \textit{ is a power of } 2$$

since the degree of $p(x)$ divides $2^n$.

**Looking back** over examples of minimal polynomials, we see:

- The cube root of 2 is not constructible, since:

$$p(x) = x^3 - 2 \text{ has degree 3, which is not a power of 2}$$

This means that a unit cube "cannot be doubled" with a construction since the sides of the doubled cube would have length $\sqrt[3]{2}$. More generally, the $n$th root of a prime number is only constructible if $n$ is a power of 2. This

- $2\cos\left(\frac{2\pi}{9}\right)$ is not constructible, since it has minimal polynomial:

$$p(x) = x^3 - 3x + 1$$

One can see this with trigonometry, or else by using the fact that $\zeta = \cos\left(\frac{2\pi}{9}\right) + i\sin\left(\frac{2\pi}{9}\right)$ has minimal polynomial $\Phi_9(x) = x^6 + x + 1$ and $2\cos\left(\frac{2\pi}{9}\right) = \zeta + \zeta^{-1}$. This has the following remarkable corollary.

**Corollary.** There is no construction that *trisects* a constructible angle.

**Proof.** $\cos\left(\frac{2\pi}{3}\right)$ is constructible and $\cos\left(\frac{2\pi}{9}\right)$ is not!

This was an open question for two thousand years!

**Exercises. 12.1.** Find the minimal polynomial of $\sqrt{2}+\sqrt{3}+\sqrt{6}$.

**12.2.** If $r>0$ is algebraic, show that $\sqrt[n]{r}$ is algebraic for all $n$.

**12.3.** Give complete constructions of the following numbers:

(a) $\frac{1}{3}$

(b) $\sqrt{3}$

(c) $\sqrt[4]{3}$

(d) $\cos\left(\frac{2\pi}{5}\right)$

(e) $\sin\left(\frac{2\pi}{5}\right)$

**12.4.** Find the intersection points of the following circles:

$$x^2+y^2=\sqrt{2}, \quad (x-1)^2+(y-1)^2=1$$

Hint: It isn't going to be pretty.

**12.5.** Prove that the angle $\theta=\frac{2\pi}{7}$ cannot be constructed.

**12.6.** Prove that the unit cube cannot be "halved" with a construction. That is, there is no construction for the lengths of the edges of a cube with volume 1/2.

**12.7.** Prove that there is no construction to *quintisect* (divide by 5) a constructible angle.