3.2 Constructible Numbers

Armed with a straightedge, a compass and two points 0 and 1 marked on an otherwise blank "number-plane," the game is to see which complex numbers you can construct, and which complex numbers you **cannot** construct!

Definition: A complex number α can be constructed if $\alpha = 0$ or $\alpha = 1$ or else α is an intersection point of a pair of lines, a line and a circle, or a pair of circles that you can draw with your straightedge and compass.

The Rules: With your straightedge and compass, you are allowed to:

(i) Draw the line $L(p, q)$ (with the straightedge) through any two points p and q that you have already constructed.

(ii) Open the compass to span the distance $|q - p|$ between any two points p and q that you have already constructed, place the base at a third point o (already constructed), and draw the circle $C(o; |q - p|)$.

Example: Your first move is one of the following:

(i) Drawing the x-axis, which is the line $L(0, 1)$, or

(ii) Drawing the circle $C(0; 1)$ (of radius 1 about 0) or else $C(1; 1)$.

When you draw all three of these, you've constructed 4 numbers:

(a) $L(0, 1)$ and $C(0; 1)$ intersect at 1 and the new number -1,

(b) $L(0, 1)$ and $C(1; 1)$ intersect at 0 and the new number 2,

(c) $C(0; 1)$ and $C(1; 1)$ intersect at the two new numbers $\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$.

Proposition 3.2.1. *All the integers can be constructed.*

Proof: By induction. 0 was given to us.

(i) 1 was given to us, and we've seen above how to construct -1.

(ii) Once you've constructed n and $-n$, draw $C(n; 1)$ and $C(-n; 1)$ to construct $n+1$ (as one point of the intersection $L(0, 1) \cap C(n; 1)$) and $-(n+1)$ (as one point of the intersection $L(0, 1) \cap C(-n; 1)$).

By induction, then, all integers can be constructed!

Construction 3.2.2. *If L is a line that has already been drawn and p is a point that has already been constructed (which may or may not be on L), then we can draw*

$$p \in L^{\perp} \quad \textit{and} \quad p \in L^{||}$$

the unique lines containing p that are perpendicular and parallel to L.

The Construction: Since L has already been drawn, there are at least two points on it that have been constructed, so in particular at least one of them is different from p. Let $q \neq p$ be one of these points. Now draw $C(p; |q-p|)$. If this circle only intersects L at q, then it is tangent to L, and $L(p,q)$ is $p \in L^{\perp}$. Otherwise let $q' \in L$ be the second point of $L \cap C(p; |q-p|)$. Now draw $C(q; |q-q'|)$ and $C(q'; |q-q'|)$. These intersect in two points r, r' and the line $L(r,r')$ is $p \in L^{\perp}$.

To draw the parallel line $p \in L^{||}$, just draw two perpendiculars. Namely, first draw $p \in L^{\perp}$, and then draw $p \in (p \in L^{\perp})^{\perp}$.

Proposition 3.2.3. *All Gaussian integers can be constructed*

Proof: To construct $a+bi$, first construct the integer a, then draw $a \in L(0,1)^{\perp}$, which is the vertical line $x = a$. Then construct any $a+bi$ on that line by induction, as in Proposition 3.2.1.

Proposition 3.2.4. *Once a complex number α has been constructed,*

$$-\alpha, \quad i\alpha, \quad \text{and} \quad \overline{\alpha}$$

can also be constructed.

Proof: Using α, construct the line $L(0,\alpha)$ and the circle $C(0; |\alpha|)$. These intersect at the two points α and $-\alpha$.

Next, recall that $i\alpha$ is the rotation of α by $\frac{\pi}{2}$. Draw $0 \in L(0,\alpha)^{\perp}$. This line intersects $C(0; |\alpha|)$ at the two points $i\alpha$ and $-i\alpha$.

If we write $\alpha = s + ti$, then $\alpha \in L(0,1)^{\perp}$ is the line $x = s$, which meets $L(0,1)$ at the real point $s + 0i$. Similarly, $\alpha \in L(0,1)^{||}$ is the line $y = t$, which meets the y-axis $L(0,i)$ at the purely imaginary point $0 + ti$. Now draw the circle $C(s+0i; |t|)$. Its intersections with $x = s$ are the two numbers α and $\overline{\alpha} = s - it$.

Proposition 3.2.5. *Once α and β have been constructed, then*

$$\alpha + \beta$$

can be constructed.

Proof: If $\alpha = 0$ or $\beta = 0$, there is nothing to do! Otherwise draw $L(0,\beta)$, the parallel line $\alpha \in L(0,\beta)^{||}$ through α, and then draw $C(\alpha; |\beta|)$. Then $\alpha \in L(0,\beta)^{||}$ and $C(\alpha, |\beta|)$ intersect at $\alpha \pm \beta$.

Construction 3.2.6. *If you can construct a length r, then you can construct $1/r$.*

If you can construct a second length s, then you can construct rs.

The Construction: First, draw the vertical "slope recorder" line:

$$1 \in L(0,1)^{\perp} \text{ (which is just the line } x = 1)$$

then draw the vertical line $r \in L(0,1)^{\perp}$ (which is $x = r$), and construct $r + i$ by intersecting $x = r$ with $C(r;1)$. Now draw $L(0, r+i)$. The intersection of this line with $x = 1$ is the point $1 + \frac{1}{r}i$, which gives $1/r$ (as the intersection of $C(0; |(1 + \frac{1}{r}i) - 1|)$ with the x-axis $L(0,1)$).

Draw the vertical line $x = s$, and construct $1 + ir$ as the intersection of the slope recorder with $C(1;r)$. Then the intersection of $L(0, 1+ir)$ (the line of slope r) with the line $x = s$ is $s + irs$, which gives rs.

Proposition 3.2.7. *Every element of the field $\mathbb{Q}(i)$ can be constructed.*

Proof: By Construction 3.2.6 and Proposition 3.2.5, we can construct every rational number, since we take any integers a and $b \neq 0$ and construct $a \times 1/b = a/b$. But the elements of $\mathbb{Q}(i)$ are all of the form $a/b + c/di$, which can then be constructed by constructing a/b and c/d, and then intersecting the line $x = a/b$ with the circle $C(a/b; |c/d|)$.

If $p \in L$ is a line passing through a point p, then we will write:

$$p \in L^{\theta}$$

for the line passing through p and making an angle θ with L, measured counterclockwise. For example, $p \in L^{\perp}$ and $p \in L^{\pi/2}$ are the same line.

Construction 3.2.8. *If $p \in L$ and $p \in L^{\theta}$ can be constructed (and drawn), then:*

(a) The "opposite" line $p \in L^{-\theta}$ can be drawn.

(b) If $q \in M$ is a point on another line, then $q \in M^{\theta}$ can be drawn.

(c) The "angle bisector" $p \in L^{\theta/2}$ can be drawn.

The Construction: Exercise!

Proposition 3.2.9. *If you can construct α, β, you can also construct*

$$1/\alpha \quad (\text{if } \alpha \neq 0) \quad \text{and} \quad \alpha \cdot \beta$$

Proof: In polar coordinates, $\alpha = (r;\theta)$ and $\beta = (s;\psi)$. Thus $L(0,\alpha)$ is the line $0 \in L(0,1)^{\theta}$ and $L(0,\beta)$ is the line $0 \in L(0,1)^{\psi}$. Then:

$$1/\alpha = (1/r; -\theta)$$

is an intersection of $0 \in L(0,1)^{-\theta}$ (drawn with Construction 3.2.8) and the circle $C(0;1/r)$ (drawn with Construction 3.2.6). Similarly,

$$\alpha\beta = (rs; \theta + \psi)$$

is an intersection of $0 \in L(0,\alpha)^{\psi}$ (drawn with Construction 3.2.8) with $C(0;rs)$ (drawn with Construction 3.2.6).

Proposition 3.2.10. *The constructible complex numbers are a* **field***:*

$$\mathbb{Q}(i) \subset F_{\text{const}} \subset \mathbb{C}$$

Proof: Additive inverses exist in F_{const}, by Proposition 3.2.6, F_{const} is closed under addition by Proposition 3.2.5, multiplicative inverses exist and F_{const} is closed under multiplication by Proposition 3.2.9, and finally F_{const} contains $\mathbb{Q}(i)$ by Proposition 3.2.7. (The associative, distributive, commutative laws are automatic since $F_{\text{const}} \subset \mathbb{C}$).

The Question: Which numbers are in F_{const} and which are not?

(This is a paraphrase of the question we asked to start this chapter)

Construction 3.2.11. *If you can construct a positive real number r, you can also construct $\sqrt{r}$.*

Remark: Pythagoras knew how to construct $\sqrt{2}$ as the hypotenuse of a right triangle. For example, $\sqrt{2} = |1+i|$, which is therefore the (positive) intersection of the circle $C(0; |1+i|)$ with the x-axis. It was apparently difficult for some of his contemporaries to accept the fact that this number was constructible but at the same time **not** rational.

The Construction: As in the Pythagorean theorem:

$$\sqrt{1+r^2} = |r+i|$$

is constructible, if r is constructible. Now consider the intersection of the circle $C(0; 1+r)$ with the vertical line $x = \sqrt{1+r^2}$, which constructs the complex number:

$$\alpha = \sqrt{1+r^2} + it$$

that therefore satisfies: $|\alpha|^2 = 1 + r^2 + t^2 = (1+r)^2$, or, simplifying:

$$t^2 = 2r$$

so that $t = \sqrt{2r}$ is constructible. We can divide by any constructed length (Construction 3.2.6), and so giving thanks to Pythagoras, we construct $\sqrt{r} = t \times 1/\sqrt{2}$.

Proposition 3.2.12. *F_{const} is closed under taking square roots.*

Proof: We need to show that if α is constructible, then $\pm\sqrt{\alpha}$ are also constructible. Again, go polar. If $\alpha = (r; \theta)$, we can bisect θ by Construction 3.2.8 to get $0 \in L(0,1)^{\theta/2}$ and we can construct the square root of r by Construction 3.2.11, and these allow us to construct

$$\pm\sqrt{\alpha} = \pm(\sqrt{r}; \frac{1}{2}\theta)$$

as the two points of the intersection of $C(0; \sqrt{r})$ with $0 \in L(0,1)^{\theta/2}$.

Remark: So far, we've concentrated on what we **can** construct. Now it is time to turn our attention to what **cannot** be constructed. This was a problem that puzzled the ancients for centuries!

In fact, with the vector space technology from §10, we will prove:

The Constructible Number Theorem: Every number α that you can construct has the following properties:

(i) α is an algebraic number.

(ii) The degree of the characteristic polynomial of α is a power of 2.

Before we prove this, we note a couple of significant corollaries:

Corollary 3.2.13. *You* **cannot** *construct* $\sqrt[3]{2}$.

Proof: $x^3 - 2$ has degree 3, which is not a power of 2!

Corollary 3.2.14. *There is no general construction for* **trisecting** *angles. (Compare with Construction 3.2.8, which bisects angles)*

Proof: Way back at the beginning, we saw how to construct $\frac{1}{2} + \frac{\sqrt{3}}{2}i$. We can subtract 1 from this to get $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$, and hence $L(0, -\frac{1}{2} + \frac{\sqrt{3}}{2}i)$, which is the same thing as the line:

$$0 \in L(0,1)^{2\pi/3}$$

If there were a general trisecting construction, we could use it to draw:

$$0 \in L(0,1)^{2\pi/9}$$

and then by intersecting with $C(0;1)$, we would have constructed:

$$\alpha = (1; \frac{2\pi}{9}) = \cos(\frac{2\pi}{9}) + \sin(\frac{2\pi}{9})i$$

But this number **cannot** be constructed. To see this, we find the characteristic polynomial of α:

$$\alpha^3 = (1; \frac{2\pi}{3}) = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \text{ and } \alpha^6 = (1; \frac{4\pi}{3}) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

so $\alpha^6 + \alpha^3 = -1$ and α is a root of $f(x) = x^6 + x^3 + 1 = 0$. Is this prime? Yes! (Exercise 8.4(g)). So $f(x)$ is the characteristic polynomial of α, and 6 isn't a power of 2, so the theorem tells us α isn't constructible! So $0 \in L(0,1)^{2\pi/9}$ cannot be drawn! So there is no way to trisect angles!!

Remark: In case you thought "of course $(1; \frac{2\pi}{9})$ isn't constructible" let me point out that $(1; \frac{2\pi}{5}) = \cos(\frac{2\pi}{5}) + \sin(\frac{2\pi}{5})i$, another unlikely-looking number, **can** be constructed. You are invited to check that:

$$(1; \frac{2\pi}{5}) = \frac{-1+\sqrt{5}}{4} + i\sqrt{\frac{5+\sqrt{5}}{8}}$$

and then to construct this with a straightedge and compass.

To prove the theorem, we will need to think about "towers" of fields.

Definition: If $E \subset F$ are fields, then $[F : E]$ is the **dimension** of F, thought of as a vector space over E.

Examples: (a) $[\mathbb{C} : \mathbb{R}] = 2$, and $[\mathbb{C} : \mathbb{Q}] = \infty$

(b) In the setting of Proposition 10.3, where $F \subset \mathbb{C}$ is a subfield and $\alpha \in \mathbb{C}$ is a root of a prime polynomial $x^d + a_{d-1}x^{d-1} + ... + a_0 \in F[x]$ then $[F(\alpha) : F] = d$, since $\{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$ is a basis of $F(\alpha)$.

Proposition 3.2.15. *If $E \subset F \subset G$ are all fields, then:*

$$[G : E] = [F : E] \cdot [G : F]$$

Proof: Let $\{f_1, ..., f_m\}$ be a basis for F as a vector space over E, and $\{g_1, ..., g_n\}$ be a basis for G as a vector space over F, and consider the set: $\{f_1 g_1, ..., f_i g_j, ..., f_m g_n\}$ of elements of G consisting of all products of pairs of basis vectors. We are done if we show that this set of mn elements is a basis of G **as a vector space over** E.

To see this, notice first of all that any $g \in G$ is a linear combination:

$$g = k_1 g_1 + ... + k_n g_n \text{ for "scalars" } k_j \in F$$

because $\{g_1, ..., g_n\}$ span G as a vector space over F. But we can also regard the scalars $k_1, ..., k_n \in F$ as **vectors** when we think of F as a vector space over E. Thus each k_j is a linear combination:

$$k_j = c_{1,j} f_1 + ... + c_{m,j} f_m \text{ for "scalars" } c_{i,j} \in E$$

Substituting for the k_j now gives us:

$$g = (c_{1,1} f_1 + ... + c_{m,1} f_m) g_1 + ... + (c_{1,n} f_1 + ... + c_{m,n} f_m) g_n$$

$$= c_{1,1} f_1 g_1 + ... + c_{i,j} f_i g_j + ... + c_{m,n} f_m g_n$$

showing that $\{f_i g_j\}$ span G as a vector space over E. And if:

$$0 = (c_{1,1} f_1 + ... + c_{m,1} f_m) g_1 + ... + (c_{1,n} f_1 + ... + c_{m,n} f_m) g_n$$

then all of the $k_j = c_{1,j} f_1 + ... + c_{m,j} f_m$ must be 0 because the $\{g_j\}$ are linearly independent, and then all of the $c_{i,j}$ must be 0 because the $\{f_i\}$ are linearly independent! Thus it follows that the $\{f_i g_j\}$ are linearly independent. So the $\{f_i g_j\}$ are a basis.

Example: Start with the field

$$F = \mathbb{Q}(\sqrt{2})$$

which is a vector space over $\mathbb{Q}$ with basis $\{1, \sqrt{2}\}$. I claim that:

$$F(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

is a vector space over F with basis $\{1, \sqrt{3}\}$. To see this, we need to check that $x^2 - 3$ is prime in $F[x]$. To see this it is enough to show that $x^2 - 3$ has no root in F. So try to solve $3 = (a + b\sqrt{2})^2 = a^2 + 2ab\sqrt{2} + 2b^2$ with $a, b \in \mathbb{Q}$. Since $\sqrt{2}$ is irrational, this would mean $2ab = 0$, so $a = 0$ or $b = 0$, but then we'd either have $a^2 = 3$ or $b^2 = \frac{3}{2}$ which is impossible since both square roots are irrational. So indeed $x^2 - 3 \in F[x]$ is prime. By the Proposition, then, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ and:

$$\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$$

is a basis of $F(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a vector space over $\mathbb{Q}$.

Proposition 3.2.16. *If F is a field with $\mathbb{Q} \subset F \subset \mathbb{C}$ and $[F : \mathbb{Q}] = n$, then every element $\alpha \in F$ is an algebraic number, and the degree of the characteristic polynomial of α divides n.*

Proof: The field $\mathbb{Q}(\alpha)$ sits between $\mathbb{Q}$ and F.

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset F$$

By Proposition 3.2.15, $[F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$. But $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is the degree of the characteristic polynomial of α.

Example (cont): (i) Let $\alpha = \sqrt{6} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The characteristic polynomial of α is $x^2 - 6$, which has degree 2 (and 2 divides 4).

(ii) Let $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The characteristic polynomial of α is $x^4 - 10x^2 + 1$, which has degree 4.

Proof of the Constructible Number Theorem: Get a notebook to go with your straightedge and compass. At the top, write:

$$F = \mathbb{Q}(i)$$

This is the field you start with, which will be updated with each new complex number that you construct. Each time you draw a line or a circle, you are constructing a finite set of new complex numbers, which are the intersection points of the line (or circle) with all the lines and circles that were drawn before. You consider these numbers one at a time and ask of each: "Is the intersection in F?" If not, update F, replacing it with a carefully chosen new field that contains the intersection point, which you enter below F in your notebook.

After going through all the lines and circles of the construction, you get a list of fields, ending with:

$$F = \mathbb{Q}(i, \alpha_1, \alpha_2, ..., \alpha_n)$$

which contains every complex number of your construction. I claim that we can choose the $\alpha_1, ..., \alpha_n$ so that:

$$[F : \mathbb{Q}] = 2^{n+1}$$

Once we prove this, we are done!. If $\alpha \in F_{\text{const}}$, then by definition there is a construction so that $\alpha \in F$, the last field in your notebook, and then Proposition 3.2.16 tells us that α is an algebraic number and that the degree of its characteristic polynomial divides $[F : \mathbb{Q}]$. So once we know that each $[F : \mathbb{Q}] = 2^{n+1}$, then we know that the characteristic polynomial of each constructible number divides a power of 2. But the only numbers that divide powers of 2 are smaller powers of 2!

To prove $[F : \mathbb{Q}] = 2^{n+1}$, we'll use Proposition 3.2.15, showing that each new field we enter into our notebook is $F(\alpha_{k+1})$, where α_{k+1} a root of a **quadratic** polynomial in $F[x] = \mathbb{Q}(i, \alpha_1, ..., \alpha_k)[x]$. That's enough, because it shows that the dimensions of:

$$\mathbb{Q}(i) \subset \mathbb{Q}(i, \alpha_1) \subset \mathbb{Q}(i, \alpha_1, \alpha_2) \subset ... \subset \mathbb{Q}(i, \alpha_1, ..., \alpha_n)$$

are $2, 2^2, 2^3, ..., 2^{n+1}$ as vector spaces over $\mathbb{Q}$. We will also see that each new α_{k+1} can be chosen to be a **real** number, from which it follows that each of the fields $\mathbb{Q}(i, \alpha_1, ..., \alpha_n)$ is closed under complex conjugation.

So let's find these quadratic polynomials. Suppose you have just drawn a line or a circle, and the field so far is $F = \mathbb{Q}(i, \alpha_1, ..., \alpha_k)$ and F is closed under complex conjugation. Then you are looking at an intersection point α, and trying to see whether it is in F or whether the new field $F(\alpha_{k+1})$ is required. One thing to notice is that since **every** number that was constructed earlier belongs to F, it follows that every line passes through two points of F and every circle has its center and a radius vector in F, **including** whatever line or circle you just drew. This means that each line is *parametrized* by:

- $\beta + \gamma x$ for some pair $\beta, \gamma \in F$ (x is a real parameter)

and the *equation* of each circle is:

- $|z - \beta|^2 = |\gamma|^2$ for some pair $\beta, \gamma \in F$ (z is a complex variable)

Also, since F is closed under conjugation, if $\beta = s + it \in F$, then:

$$\overline{\beta},\ \beta\overline{\beta} = s^2 + t^2,\ \frac{1}{2}(\beta + \overline{\beta}) = s \text{ and } \frac{1}{2i}(\beta - \overline{\beta}) = t$$

are also all in F, and similarly for γ.

Now let's consider the three possibilities for α:

1) α is an intersection of two lines L_1 and L_2:

$$\beta_1 + \gamma_1 x = \alpha = \beta_2 + \gamma_2 x_2$$

Let $\beta_1 = s_1 + it_1, \beta_2 = s_2 + it_2$, $\gamma_1 = u_1 + iv_1$ and $\gamma_2 = u_2 + iv_2$. Then α is obtained by solving the pair of linear equations:

$$s_1 + u_1 x_1 = s_2 + u_2 x_2$$

$$t_1 + v_1 x_1 = t_2 + v_2 x_2$$

which can easily be done. Namely:

$$x = \frac{v_2(s_2 - s_1) + u_2(t_1 - t_2)}{u_1 v_2 - v_1 u_2}$$

(if $u_1 v_2 - v_1 u_2 = 0$, the lines are parallel). This is an element of F! And this means that α is also in F:

$$\alpha = \beta + \gamma \frac{v_2(s_2 - s_1) + u_2(t_1 - t_2)}{u_1 v_2 - v_1 u_2}$$

so in this case we don't add a new entry to our notebook.

2) α is an intersection of a line and a circle L_1 and C_2:

$$\alpha = \beta_1 + \gamma_1 x \quad \text{and} \quad |\alpha - \beta_2|^2 = |\gamma_2|^2$$

Write out $\beta_1, \beta_2, \gamma_1$ and γ_2 as in 1). Then substitute:

$$|(\beta_1 + \gamma_1 x) - \beta_2|^2 = |\gamma_2|^2$$

$$(s_1 + u_1 x - s_2)^2 + (t_1 + v_1 x - t_2)^2 = u_2^2 + v_2^2$$

and expand, to get a quadratic polynomial:

$$ax^2 + bx + c = 0, \quad \text{where}$$

$a = (u_1^2 + v_1^2)$

$b = 2(u_1(s_1 - s_2) + v_1(t_1 - t_2))$

$c = (s_1 - s_2)^2 + (t_1 - t_2)^2 - (u_2^2 + v_2^2)$

The roots of this polynomial are the values of x so that $\alpha = \beta + \gamma x$ is a point of intersection of the line and circle. This is a quadratic polynomial with real coefficients, and its roots have to be real numbers (if the roots weren't real, then the line would not intersect the circle!!) It is possible that the roots of this polynomial are already in F, in which case, as before, we don't make a new entry in the notebook, because then $\alpha \in F$. If the roots aren't in F, let α_{k+1} be one of them and then $\alpha = \beta + \gamma\alpha_{k+1} \in F(\alpha_{k+1})$ as we wanted. So we make $F(\alpha_{k+1})$ the new entry in the notebook.

3) α is an intersection of two circles C_1 and C_2:

$$|\alpha - \beta_1|^2 = |\gamma_1|^2 \text{ and } |\alpha - \beta_2|^2 = |\gamma_2|^2$$

Let $\alpha = x + iy$ and write out $\beta_1, \beta_2, \gamma_1, \gamma_2$ as in 1). Then we solve:

$$(x - s_1)^2 + (y - t_1)^2 = u_1^2 + v_1^2 \text{ and } (x - s_2)^2 + (y - t_2)^2 = u_2^2 + v_2^2$$

and subtracting the first from the second, we get:

$$(*)\ 2(s_1 - s_2)x + 2(t_1 - t_2)y = (u_2^2 + v_2^2 + s_1^2 + t_1^2) - (u_1^2 + v_1^2 + s_2^2 + t_2^2)$$

Solve for y in $(*)$ and substitute back into the first equation to get a quadratic polynomial (which I won't write in all the gory details!)

$$ax^2 + bx + c = 0 \text{ with } a, b, c \in F$$

As before, the roots have to be real, or else the circles don't intersect. The roots might be in F, in which case the intersections are all in F. Otherwise we get out our notebook and add $F(\alpha_{k+1})$ where α_{k+1} is a root of $ax^2 + bx + c$. In this case, α_{k+1} is the x-coordinate of the intersection, and we can use $(*)$ to solve for the y-coordinate, which is then also in $F(\alpha_{k+1})$. Thus $\alpha \in F(\alpha_{k+1})$, and this finishes the proof!

3.2.1 Constructible Number Exercises

11-1 Explain how to do the three constructions of Construction 3.2.8.

11-2 Construct the following lengths from scratch:

(a) $\sqrt{7}$

(b) $\sqrt{2 - \sqrt{2}}$

(c) $\sqrt{\frac{5+\sqrt{5}}{8}}$

11-3 Construct the following complex numbers:

(a) $(1; \frac{\pi}{6}) = \cos(\frac{\pi}{6}) + \sin(\frac{\pi}{6})i$

(b) $(1; \frac{2\pi}{5}) = \cos(\frac{2\pi}{5}) + \sin(\frac{2\pi}{5})i$

(c) $(1; \frac{\pi}{12}) = \cos(\frac{\pi}{12}) + \sin(\frac{\pi}{12})i$

11-4 Find the characteristic polynomial of $(1; \frac{2\pi}{7}) = \cos(\frac{2\pi}{7}) + \sin(\frac{2\pi}{7})i$. Conclude from the constructible number theorem that this cannot be constructed, so general angles cannot be "heptasected" (divided by 7).

11-5 Find the characteristic polynomial of $(1; \frac{2\pi}{25}) = \cos(\frac{2\pi}{25}) + \sin(\frac{2\pi}{25})i$. Conclude that this cannot be constructed, so general angles cannot be "pentasected" (divided by 5).

11-6 For which n can $\sqrt[n]{2}$ be constructed? What about $\sqrt[n]{3}$?