NOTES AND EXERCISES ON CONSTRUCTIBILITY

In what follows, we identify the euclidean plane with the set of complex numbers $\mathbb{C}$. All fields are assumed to be subfields of $\mathbb{C}$.

A field is *constructible* if it is closed under square roots and under complex conjugation.

Let $\mathcal{C}$ be a set of points, lines, and circles satisfying the axioms of constructibility (given in class) that is, a constructible collection. The members of $\mathcal{C}$ are called constructible points, resp. lines, resp. circles. We showed in class that:

$(*)$ The constructible points form a constructible field.

The following exercises lead to the conclusion that this actually gives a one-one correspondence between constructible collections and constructible fields.

(a) Prove that a constructible line contains two constructible points.

(b) Prove that the center of a constructible circle is constructible, and also that there is a constructible point lying on the circle.

(c) Prove that on any constructible circle there lie infinitely many constructible points.

(d) Explain why (a) and (b) show that the set of lines (respectively circles) in $\mathcal{C}$ is completely determined by the set of points in $\mathcal{C}$.

(e) Given real numbers a, b, c, and d, not all 0, show that the set of points $(x, y) \in \mathbb{R}^2$ satisfying the relation

$$a(x^2 + y^2) + bx + cy + d = 0$$

are all the points in a set of one of the following types:

(i) The empty set;
(ii) A set consisting of one point;
(iii) A line;
(iv) A circle.

Show conversely that any set of one of the preceding types is defined by a relation of the given form.

(f) Let e be any one of a, b, c, d which is not zero. In cases (ii), (iii), and (iv) above, show that the set is constructible if and only if the ratios a/e, b/e, c/e, and d/e are all constructible.

(g) Let F be a constructible field. Prove that the points of F together with all the lines joining pairs of points in F together with all the circles whose center is in F and which pass through at least one point of F form a constructible collection.

Theorem 1. *There is a* one-one correspondence *between constructible collections and constructible fields, obtained by associating to each constructible collection its set of points.*

Proof. This follows from $(*)$, (d) and (g).

Corollary. *For a set $F \subset \mathbb{C}$ let $\mathcal{C}_F$ be the least constructible collection containing F. Then the points of $\mathcal{C}_F$ form the smallest constructible field containing F.*

(OVER)

Say that a point P (i.e., a complex number) is "constructible from F" if $P \in \mathcal{C}_F$.

Theorem 2. *Let F be a field which is closed under complex conjugation. A point P is constructible from F if and only if it "sits in a quadratic tower based on F," by which is meant that there exists a sequence of fields*

$$F = F_0 \subset F_1 \subset \cdots \subset F_n$$

such that $[F_i : F_{i-1}] = 2$ for all $i = 1, 2, \ldots, n$ and such that $P \in F_n$.

Corollary. *If P is constructible from F then $[F(P) : F]$ is a power of 2.*

Remarks. 1. P sits in a quadratic tower if and only if

$$P \in F[x_1, x_2, \ldots, x_n]$$

where $x_i^2 \in F[x_1, x_2, \ldots, x_{i-1}]$ for $1 \le i \le n$. That's because any degree-2 extension of a field K is obtained by adjoining the root of a quadratic equation, hence (as long as K has characteristic $\neq 2$) by adjoining the square root of some element of K.

Roughly speaking, for P to sit in a quadratic tower means that P can be constructed starting with an element of F and applying addition, subtraction, multiplication, division, and square root a finite number of times. (And, recall, each of these operations can be done with straightedge and compass.)

2. Let z be a root of the polynomial $X^4 + X + 1 = 0$, and set $F = \mathbb{Q}[z]$. Then the complex conjugate $\bar{z}$ is constructible from F (since $\mathcal{C}_F$ is closed under complex conjugation), and it is a root of the polynomial $(X^4 + X + 1)/(X - z) \in F[X]$. It can be shown that this polynomial is irreducible over F, and so $[F(\bar{z}) : F] = 3$. Thus $\bar{z}$ cannot sit in any quadratic tower based on F.

This doesn't contradict the Theorem, because F is not closed under complex conjugation.

Proof of Theorem 2. ($\Rightarrow$) Since the set of points in $\mathcal{C}_F$ is closed under square roots, Remark 1 shows that every F_n as above is contained in that set of points. Thus any $P \in F_n$ is constructible from F.

($\Leftarrow$) It suffices to show that the set G of all points which sit in some quadratic tower form a constructible field—since that forces $\mathcal{C}_F$ (the smallest constructible field containing F) to be contained in G.

First, if P sits in a quadratic tower, then so does its complex conjugate, as one can see by applying conjugation to the entire tower. (This is where we use that F is closed under conjugation.) Thus G is closed under conjugation.

Next, suppose that P and Q are in G, so that as in Remark 1,

$$P \in F[x_1, x_2, \ldots, x_n], \qquad Q \in F[y_1, y_2, \ldots, y_m].$$

Then we have the quadratic tower obtained from F by first adjoining the x's one at a time, and then adjoining the y's one at a time. Both P and Q are in the top level of this tower, whence so is $P + Q$, so that $P + Q \in G$. Similarly PQ and (if $Q \neq 0$) P/Q are members of G. This shows that G is a field.

If P sits in some tower $F = F_0 \subset \cdots \subset F_n$, then $\sqrt{P}$ sits in the tower $F = F_0 \subset \cdots \subset F_n \subset F_n(\sqrt{P})$. Thus G is closed under square roots. □

Here is a variant of Theorem 1, closer to the discussion in Dummit and Foote.

Theorem 1′. *There is a* one-one correspondence *between constructible collections and subfields of $\mathbb{R}$ closed under square roots, obtained by associating to each constructible collection the least field containing the (real) coordinates of all its points.*

Proof. One could imitate the proof of Theorem 1, *mutatis mutandis.* Or, if Theorem 1 is assumed then one can use the easily-shown fact that by associating to each constructible field F the field $G := F \cap \mathbb{R}$, one gets a one-one correspondence between constructible fields and subfields of $\mathbb{R}$ closed under square roots. (Show that $a + ib \in F \iff a \in G$ and $b \in G$, and conclude that $F = G[i]$.)