HISTORY OF MATHEMATICS
MATHEMATICAL TOPIC X
FIELDS

PAUL L. BAILEY

1. Fields

Definition 1. A *field* is a set F together with operations
$$+ : F \times F \to F \text{ and } \cdot : F \times F \to F$$
satisfying

(F1) $a + b = b + a$ for every $a, b \in F$;
(F2) $(a + b) + c = a + (b + c)$ for every $a, b, c \in F$;
(F3) there exists $0_F \in F$ such that $a + 0_F = a$ for every $a \in F$;
(F4) for every $a \in F$ there exists $b \in F$ such that $a + b = 0_F$;
(F5) $ab = ba$ for every $a, b \in F$;
(F6) $(ab)c = a(bc)$ for every $a, b, c \in F$;
(F7) there exists $1_F \in F$ such that $a \cdot 1_F = a$ for every $a \in F$;
(F8) for every $a \in F \smallsetminus \{0_F\}$ there exists $c \in F$ such that $ac = 1_F$;
(F9) $a(b + c) = ab + ac$ for every $a, b, c \in F$;

Definition 2. Let F be a field. A *subfield* of F is a subset $S \subset F$ such that
(S0) $1 \in S$;
(S1) $a, b \in S \Rightarrow a + b \in S$;
(S2) $a \in S \Rightarrow -a \in S$;
(S3) $a, b \in S \Rightarrow ab \in S$;
(S4) $a \in S \Rightarrow a^{-1} \in S$.

If S is a subfield of F, we write $S \leq F$.

Remark 1. Properties **(S0)** through **(S4)** imply that a subfield of F is a subset of F which is itself a field.

Problem 1. Let F be a field and $\mathcal{S}$ be a collection of subfields of F.
Show that $\cap\mathcal{S} \leq F$.

Definition 3. Let $A \subset F$. The *subfield of F generated by A*, denoted by $\mathrm{gf}_F(A)$, is the intersection of all subfields of F which contain A.

If S is a subfield of F and $A \subset F$. let $S(A)$ denote the subfield of F generated by $S \cup A$. If $A = \{\alpha_1, \dots, \alpha_n\}$ is finite, let $S(\alpha_1, \dots, \alpha_n) = S(A)$. In particular, if $a \in F$, let $S(a) = S(\{a\})$.

Remark 2. Every subfield of $\mathbb{C}$ contains $\mathbb{Q}$, so every subfield generated by a subset of $\mathbb{C}$ contains $\mathbb{Q}$.

Example 1. Let $\alpha = \sqrt{2}$. Then
$$\mathbb{Q}(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Q}\}.$$

Date: December 13, 2004.

2. Polynomials

Definition 4. Let F be a field. A *polynomial over* F is a function $f : F \to F$ of the form
$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n,$$
where n is a nonnegative integer and $a_i \in F$ for $i = 1, \ldots, n$, with $a_n \neq 0$ (unless $f(X) = 0$). We call the variable X an *indeterminate*.

The number n is called the *degree* of f, and is denoted by $\deg(f)$, The elements a_i are called the *coefficients* of f.

The number a_n is called the *leading coefficient*. We say that f is *monic* if $a_n = 1$.

The element a_0 is called the *constant coefficient*. The polynomials of degree zero are called *constants*, and are identified with the elements of the field F. By convention, $\deg(0) = -\infty$.

The set $F[X]$ is closed under addition, subtraction, and multiplication.

Proposition 1 (Division Algorithm for Polynomials)**.** *Let F be a field and let $f, g \in F[X]$. Then there exist polynomials $q, r \in \mathbb{F}[X]$ such that*
$$g = qf + r \qquad \textit{such that} \qquad \deg(r) < \deg(f).$$
If f and g are monic, then q and r may be chosen to be monic or zero.

Proof. Without loss of generality, assume that f and g are monic. Let
$$S = \{h \in F[X] \mid h = g - qf \text{ for some monic } q \in F[X]\}.$$
Clearly S is nonempty; let $r \in S$ be a polynomial of minimal degree in S, so that $r = g - qf$ for some monic $q \in F[X]$. Then $g = qf + r$.

We claim that $\deg(r) < \deg(f)$, To see this, let $k = \deg(r) - \deg(f)$, and assume that $k \geq 0$. Then $X^k \in F[X]$, and $h = r - X^k f = g - (q - X^k)f \in S$ is a monic polynomial of degree less than that of r, contradicting the selection of r. $\square$

Definition 5. Let F be a field and let $f, g \in F[X]$ We say that g is *divisible* by f, or that f is a *factor* of g, or that f *divides* g, and write $f \mid g$, if there exists $k \in F[X]$ such that $g = fk$. We see that f divides g if and only if the remainder upon division of g by f is $r = 0$.

Definition 6. Let F be a field, $f \in F[X]$, and $\alpha \in F$. If $\alpha \in F$, we say that α is a *zero* of f if $f(\alpha) = 0$. In this case, we say that f *annihilates* α.

Proposition 2 (Remainder Theorem)**.** *Let F be a field, $f \in F[X]$, and $\alpha \in F$. Let $h(X) = (X - \alpha) \in F[X]$. Write $f = hq + r$, where $\deg(r) < \deg(h)$. Then $r \in F$, and $f(\alpha) = r$.*

Proposition 3 (Factor Theorem)**.** *Let F be a field, $f \in F[X]$, and $\alpha \in F$. Let $h(X) = (X - \alpha) \in F[X]$. Then $h \mid f$ if and only if $f(\alpha) = 0$.*

Proposition 4. *Let F be a field and let $\alpha \in F$. Suppose that $g = fq$ for some $f, g, q \in F[X]$, and that $g(\alpha) = 0$. Then either $f(\alpha) = 0$ or $q(\alpha) = 0$.*

Definition 7. Let $f, g \in F[X]$. A *greatest common divisor* of m and n, denoted $\gcd(m, n)$, is a monic $d \in F[X]$ such that

(a) $d \mid f$ and $d \mid g$;
(b) If $e \mid f$ and $e \mid g$, then $e \mid d$.

Proposition 5 (Euclidean Algorithm for Polynomials)**.** *Let $f, g \in F[X]$. Then there exists $d \in F[X]$ such that $d = \gcd(m, n)$, and there exist $s, t \in F[X]$ such that*

$$d = sf + tg.$$

If f and g are monic, we may choose s and t to be monic.

Proof. Without loss of generality, assume that f and g are monic. Let

$$S = \{h \in F[X] \mid h = sf + tg \text{ for some monic } s, t \in F[X]\}.$$

Clearly S is nonempty; select $d \in S$ of minimal degree, so that $d = sf + tg$ for some monic $s, t \in F[X]$.

Now $f = qd + r$ for some monic $q, r \in F[X]$ with $\deg(r) < \deg(d)$. Then $f = q(sf + tg) + r$, so $r = (1 - qs)f + (qt)g \in S$. If r is nonzero, this contradicts the selection of d; thus $r = 0$, which shows that $d \mid f$. Similarly, $d \mid g$.

If $e \mid f$ and $e \mid g$, then $f = ke$ and $g = le$ for some $k, l \in F[X]$. Then $d = ske + tle = (sk + tl)e$. Therefore $e \mid d$. This shows that $d = \gcd(m, n)$. $\square$

Definition 8. Let F be a field and let $f \in F[X]$. We say that f is *irreducible over F* if whenever $f = gh$ for some $g, h \in F[X]$, either $\deg(g) = 1$ or $\deg(h) = 1$.

Example 2. If $\deg(f) \in \{2, 3\}$, then f is irreducible over F if and only if f has no zero in F.

3. Field Extensions

Definition 9. A *field extension E/F* consists of a field E which contains a field F.

Definition 10. Let E/F be a field extension, and let $\alpha \in E$. We say that α is *algebraic* over F if there exists a nonzero polynomial $f \in F[X]$ such that $f(\alpha) = 0$. Otherwise, we say that α is *transcendental* over F.

Proposition 6. *Let E/F be a field extension and let $\alpha \in E$ be algebraic over F. Then there exists a unique monic irreducible polynomial $f \in F[X]$ such that $f(\alpha) = 0$.*

Proof. Since α is algebraic over F, there exists some polynomial in $F[X]$ which annihilates α. Let $f \in F[X]$ be a nonzero polynomial of minimal degree which annihilates α. Clearly f is irreducible, since it is of minimal degree. We may divide by the leading coefficient to see that we may select f to be monic. Now suppose that g is another monic polynomial of minimal degree which annihilates α. We have $\deg(f) = \deg(g)$. Then $\deg(f - g) < \deg(f) = \deg(g)$. Since f is of minimal degree among nonzero polynomials which annihilate α, we must have $f - g = 0$. Thus $f = g$, and f is unique. $\square$

Definition 11. Let E/F be a field extension and let $\alpha \in E$ be algebraic over F. The *minimum polynomial* of α over F, denoted $\text{minpoly}(\alpha/F)$, is the unique monic irreducible polynomial which annihilates α. The *degree* of α over F, denoted $\deg(\alpha/F)$, is equal to $\deg(\text{minpoly}(\alpha/F))$.

Definition 12. Let E/F be a field extension and let $\alpha \in E$. The *evaluation map* on $F[X]$ with respect to α is the function $\psi_\alpha : F[X] \to E$ defined by $f \mapsto f(\alpha)$. The image of the evaluation map is denoted $F[\alpha]$; that is,

$$F[\alpha] = \psi_\alpha(F[X]) = \Big\{ \sum_{i=0}^{k} a_i \alpha^i \mid k \in \mathbb{N}, a_i \in F \Big\} \subset E.$$

Proposition 7. *Let E/F be a field extension and let $\alpha \in E$. If α is transcendental over F if and only if ψ_α is injective.*

Proof. Suppose that α is transcendental. Let $f, g \in F[X]$ so that $f(\alpha)$ and $g(\alpha)$ are arbitrary members of $F[\alpha]$. Suppose that $f(\alpha) = g(\alpha)$; then $(f - g)(\alpha) = 0$, so $(f - g)$ is a polynomial which annihilates α. Since α is transcendental, we must have $f - g = 0$, so $f = g$.

On the other hand, if α is not transcendental, it is algebraic; let $f = \operatorname{minpoly}(\alpha/F)$. Then $\psi_\alpha(f) = \psi_\alpha(0)$, and ψ_α is not injective. □

Proposition 8. *Let E/F be a field extension and let $\alpha \in E$. Let $F[\alpha] = \psi_\alpha(F[X])$ denote the image of $F[X]$ under the evaluation map. Let α is algebraic over F and $\deg(\alpha/F) = n$, then $F[\alpha] = S$, where*

$$S = \Big\{ \sum_{i=0}^{n-1} a_i \alpha^i \mid a_i \in F \Big\};$$

moreover, $F[\alpha]$ is a field, and $F[\alpha] = F(\alpha)$.

Proof. Clearly all elements of the form $\sum_{i=0}^{n-1} a_i \alpha^i$ are in $F[\alpha]$, so $S \subset F[\alpha]$.

Let $f \in F[X]$ be the minimum polynomial of α over F. Let $g \in F[X]$; then $g(\alpha)$ is an arbitrary member of $F[\alpha]$. Now $g(X) = f(X)q(X) + r(X)$, where $\deg(r) < \deg(f)$. By the remainder theorem, $g(\alpha) = f(\alpha)q(\alpha) + r(\alpha) = r(\alpha) \in S$.

Since $F[X]$ is closed under addition, subtraction, and multiplication, so is $F[\alpha]$. We only need to show that $f(\alpha)$ if invertible for $f(\alpha) \neq 0$.

Let $\beta \in F[\alpha]$. Then $\beta = g(\alpha)$ for some $g \in F[X]$; by the division algorithm, we may select g so that $\deg(g) < \deg(f)$. Since f is irreducible, we see that $\gcd(f, g) = 1$, so there exist $s, t \in F[X]$ such that $sf + tg = 1$. Then $t(\alpha)g(\alpha) = 1$, so $\beta^{-1} = t(\alpha)$, and β is invertible. □

4. Vector Spaces

Definition 13. Let F be a field. A *vector space* over F is a set V together with operations

$$+ : V \times V \to V \quad \text{and} \cdot : F \times V \to V$$

satisfying

(V1) $v + w = w + v$ for all $v, w \in V$;
(V2) $v + (w + x) = (v + w) + x$ for all $v, w, x \in V$;
(V3) there exists $0_V \in V$ such that $v + 0_V = v$ for all $v \in V$;
(V4) for every $v \in V$ there exists $w \in V$ such that $v + w = 0_V$;
(V5) $1_F \cdot v = v$ for every $v \in V$;
(V6) $(ab)v = a(bv)$ for every $v \in V$ and $a, b \in F$;
(V7) $(a + b)v = av + bv$ for every $v \in V$ and $a, b \in F$.
(V8) $a(v + w) = av + aw$ for every $v, w \in V$ and $a \in F$;

Problem 2. Let V be a vector space over a field F. Let $a \in F$ and $x \in V$.
(a) Show that $0_F \cdot x = 0_V$.
(b) Show that $a \cdot 0_V = 0_V$.
(c) Show that $(-1_F) \cdot x = -x$.

Definition 14. Let V be a vector space over a field F.
A *subspace* of V is a subset $W \subset V$ such that
(W0) $0_V \in W$;
(W1) $x, y \in W \Rightarrow x + y \in W$;
(W2) $a \in F, x \in W \Rightarrow ax \in W$.
If W is a subspace of V, this is denoted by $W \leq V$.

Remark 3. Properties **(W0)** through **(W2)** imply that a subspace of V is a subset of V which is itself a vector space.

Problem 3. Let V be a vector space over a field F and let $\mathcal{W}$ be a collection of subspaces of V.
Show that $\cap\mathcal{W} \leq V$.

Definition 15. Let V be a vector space over a field F and let $A \subset V$. The *subspace of* V *generated by* A, denoted $\mathrm{gv}_V(A)$, the intersection of all subspaces of V which contain A. This subspace is called the *span* of A.

Problem 4. Let V be a vector space over a field F and let $A = \{v_1, \dots, v_n\}$. Show that

$$\mathrm{gv}_V(A) = \Big\{ \sum_{i=1}^{n} a_i v_i \mid a_i \in F \Big\}.$$

5. Vector Space Dimension

Definition 16. Let V be a vector space over a field F. Let $B \subset V$.

We say that B *spans* V is for every $x \in V$ there exist $a_1, \ldots, a_n \in F$ and $v_1, \ldots, v_n \in B$ such that $x = \sum_{i=1}^{n} a_i v_i$.

We say that B is *linearly independent* if whenever $v_1, \ldots, v_n \in B$ are distinct elements of B and $a_1, \ldots, a_n \in F$,

$$\sum_{i=1}^{n} a_i v_i = 0 \Rightarrow a_i = 0 \text{ for } i = 1, \ldots, n.$$

We say that B is a *basis* for V if B spans V and is linearly independent.

Problem 5. Let V be a vector space over a field F and let $X \subset V$ span V. Show that $V = \mathrm{gv}_V(X)$.

Problem 6. Let V be a vector space over a field F and let $X \subset V$ be linearly independent. Let $v \in X$. Show that $\mathrm{gv}_V(X \smallsetminus \{v\})$ is a proper subset of $\mathrm{gv}_V(X)$.

Problem 7. Let V be a vector space over a field F and let $X \subset V$ span V. Show that there exists a subset $B \subset X$ such that B is a basis for V.

Problem 8. Let V be a vector space over a field F and let $X \subset V$ be linearly independent. Show that there exists a subset $Y \subset V$ such that $X \cup Y$ is a basis for V.

Problem 9. Let V be a vector space over a field F. Let $A = \{v_1, \ldots, v_m\}$ and $B = \{w_1, \ldots, w_n\}$ be bases for V. Show that $m = n$.

Definition 17. Let V be a vector space over a field F. If V has a basis containing n elements, where $n \in \mathbb{N}$, we say that V is *finite dimensional*, and that n is the *dimension* of V; this is denoted by $\dim(V) = n$.

Problem 10. Let V be a vector space over a field F and let $U, W \leq V$. Set $U + W = \{u + w \mid u \in U, w \in W\}$.
(a) Show that $U + W \leq V$.
(b) Show that $\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W)$.

Problem 11. Let F be a field and let n be a positive integer. Let F^n denote the cartesian product of F with itself n times. Show that F^n is a vector space over F of dimension n.

Observation 1. Let E/F be a field extension. We may add the elements of E, and multiply them by elements of F. In this way, we may view E as a vector space over F.

Definition 18. Let E/F be a field extension. The *degree* of the extension, denoted $[E : F]$, is its dimension of E as a vector space over F.

6. Types of Extensions

Definition 19. Let E/F be a field extension.

We say that E/F is a *primitive extension* if $E = F[\alpha]$ for some $\alpha \in E$ which is algebraic over F.

We say that E/F is a *finite extension* if $[E : F] < \infty$.

We say that E/F is a *algebraic extension* if every element of E is algebraic over F.

Proposition 9. *Let E/F be a primitive extension such that $E = \mathbb{F}[\alpha]$, where α is algebraic over F with* $\text{minpoly}(\alpha/F) = f \in F[X]$. *Let $n = \deg(f)$. Then the set*

$$B = \{1, \alpha, \ldots, \alpha^{n-1}\}$$

is a basis for E/F, and in particular, $[E : F] = n$.

Proof. Since $E = F[\alpha]$, that B spans E is a direct consequence of Proposition **??**. To see that B is linearly independent, let

$$a_0 \cdot 1 + a_1\alpha + \cdots + a_n\alpha^{n-1} = 0$$

be a dependence relation. Then α is a root of the polynomial $\sum_{i=1}^{n-1} a_i X^i$. Since this polynomial has lower degree than f, it must be the zero polynomial, so $a_i = 0$ for every i. This shows that B is linearly independent over F. □

Proposition 10. *Let E/F be a finite extension. Then E/F is an algebraic extension.*

Proof. Let $[E : F] = n$, and let $\alpha \in E$. The set $S = \{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ contains $n + 1$ elements, and so it must be linearly dependent over F. Thus there exists a nontrivial dependence relation

$$a_0 \cdot 1 + a_1\alpha + \cdots + a_n\alpha^n = 0.$$

Let $f(X) = a_0 + a_1X + \ldots a_nX^n$. Then $f(\alpha) = 0$, so α is algebraic over F. □

Proposition 11. *Let K/E and E/F be finite field extensions of dimension n and m respectively. If $\{z_1, \ldots, z_n\}$ is a basis for K/E and $\{y_1, \ldots, y_m\}$ is a basis for K/F, then $\{y_iz_j \mid i = 1, \ldots, m;\ j = 1, \ldots, n\}$ is a basis for K/F. In particular, K/F is finite, and*

$$[K : F] = [K : E][E : F].$$

Proof. Let $\alpha \in K$. Then α is in the span of $\{z_j\}$, so $\alpha = \sum_{j=1}^{n} b_jz_j$ for some $b_j \in E$. Since each $b_j \in E$, it is in the span of $\{y_i\}$, so $b_j = \sum_{i=1}^{m} a_{ij}y_i$ for some $a_{ij} \in F$. Thus

$$\alpha = \sum_{j=1}^{n} \Big[\sum_{i=1}^{m} a_{ij}y_i \Big] z_j = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}y_iz_j.$$

Thus $\{y_iz_j\}$ spans K.

Now consider a dependence relation $\sum_{j=1}^{n} \sum_i i = 1^m a_ijy_iz_j = 0$. Collect like terms to obtain $\sum_{j=1}^{n} \left[\sum_{i=1}^{m} a_{ij}y_i \right] z_j = 0$. Since $\{z_j\}$ is linearly independent, we must have $\sum_{i=1}^{n} a_{ij}y_i = 0$ for every j. But since $\{y_i\}$ is linearly independent, this implies that $a_{ij} = 0$ for every i and j. Thus $\{y_iz_j\}$ is linearly independent over F. □

7. Field of Constructible Numbers

Definition 20. Let $S \subset \mathbb{C}$ and set $z \in \mathbb{C}$. We say that a line $L \subset \mathbb{C}$ is constructible from S if $L \cap S$ contains at least two points. We say that a circle $C \subset \mathbb{C}$ is constructible from S if the center of C is in S and $C \cap S$ is nonempty. We say a point $z \in \mathbb{C}$ is constructible from S if one of the following conditions holds:

- **(C0)** $z \in S$;
- **(C1)** $z \in L_1 \cap L_2$, where L_1 and L_2 are lines constructible from S;
- **(C2)** $z \in L_1 \cap C_1$, where L_1 is a line and C_1 is a circle constructible from S;
- **(C3)** $z \in C_1 \cap C_2$, where C_1 and C_2 are circles constructible from S.

Let $C(S)$ be the set of points which are constructible from S.

Set $C_0(S) = S$ and inductively set $C_{n+1}(S) = C(C_n(S))$. Let $S = \{0, 1\} \in \mathbb{C}$, and define

$$\mathbb{K} = \cup_{n=0}^{\infty} C_n(S);$$

members of $\mathbb{K}$ are called *constructible numbers*.

Proposition 12. *Let $a, b \in \mathbb{K}$. Then*

- **(K1)** $a + b \in \mathbb{K}$*;*
- **(K2)** $-a \in \mathbb{K}$*;*
- **(K3)** $ab \in \mathbb{K}$*;*
- **(K4)** $a^{-1} \in \mathbb{K}$ *if* $a \neq 0$*;*
- **(K5)** $\pm\sqrt{a} \in \mathbb{K}$*;*
- **(K6)** $\overline{a} \in \mathbb{K}$*;*

Thus the set $\mathbb{K}$ is a subfield of $\mathbb{C}$ which is closed under square roots and conjugation.

Proof. Note that $a+b$ is the fourth point in a parallelogram with points a, 0, and b; we have seen that this construction is possible. Also, $-a$ is the intersection of the line through 0 and a with the circle centered at 0 through a, so $-a$ is constructible.

Let $a = re^{i\theta}$ be the polar expression of a. Now $r = |a|$; this may be constructed by intersecting the real axis with the circle centered at 0 through a.

Now let $a = re^{i\theta}$ and $b = se^{i\gamma}$; then $ab = rse^{i(\theta+\gamma)}$. We have seen that if we can construct lengths r and s, then we can construct the length rs. We only need to show that we can construct the angle $\theta + \gamma$. Try to do this geometrically; otherwise it will follow algebraically from the similar facts for the real and imaginary parts of a and b.

Next we describe how to construct the conjugate $\overline{a}$ of a. Form the line perpendicular to the real axis and passing through a. Intersect this line with the circle centered at 0 through a. One point of intersection is a, the other is $\overline{a}$.

Consider that $a^{-1} = \frac{1}{r}e^{-i\theta}$. We have seen that we can construct $\frac{1}{r}$, and we can bisect any angle. Thus $a^{-1} \in \mathbb{K}$. $\square$

Proposition 13. *Let $z \in \mathbb{C}$. Then $z \in \mathbb{K}$ if and only if $\Re z \in \mathbb{K}$ and $\Im z \in \mathbb{K}$. In particular, i is constructible.*

Proof. Note that the real axis is immediately constructible from $\{0, 1\}$, and the imaginary axis is constructible as the perpendicular to the real axis through 0.

Suppose that $z \in \mathbb{K}$. Then $|z|$ is the positive real number obtained as the intersection of real line and the circle centered at 0 and through z. Then $|z|^2$ is constructible since $\mathbb{K}$ is a field, and since $z\overline{z} = |z|^2$, we see that $\overline{z} = \frac{|z|^2}{z}$ is constructible. Thus $\Re z = \frac{1}{2}(z + \overline{z})$ is constructible, and $\Im z = z - \Re z$ is constructible.

Suppose that $\Re z$ and $\Im z$ are constructible. Now i is the intersection of the unit circle and the imaginary axis, so i is constructible. Thus $z = \Re z + i\Im z$ is constructible. □

8. Constructed Fields

Definition 21. Let $\mathbf{z} = (z_1, \dots, z_n)$ be an n-tuple of complex numbers. We say that $\mathbf{z}$ is *constructed* if $z_1 = i$ and $z_{i+1} \in C(\mathbb{Q}[z_1, \dots, z_i])$ for $i = 1, \dots, n$. If $F \leq \mathbb{C}$, we say that F is constructed if $F = \mathbb{C}[z_1, \dots, z_n]$ for some constructed tuple $(z_1, \dots, z_n)$.

Proposition 14. *Let $F \leq \mathbb{C}$ and $z \in \mathbb{C}$. Suppose $i \in F$. Then $z \in F$ if and only if $\Re z, \Im z \in F$. In this case, $\overline{z} \in F$ and $|z|^2 \in F$.*

Proof. Let $z = x + iy$, where $x, y \in \mathbb{R}$. If $x, y, i \in F$, then obviously $z \in F$.

Suppose $z, i \in F$; then $z - iz \in F$. Now $z - iz = (x - ix) - (y - iy) = (x - y)(1 - i)$. Since $i \in F$, $1 - i \in F$, so $x - y \in F$. Now $(x - y) - z = y - iy = y(1 - i)$, so $y \in F$. Thus $x \in F$. Now $\overline{z} = x - iy \in F$, so $|z|^2 = z\overline{z} \in F$. □

Proposition 15. *If $\alpha \in \mathbb{K}$, then there exists a constructed tuple $(z_1, \dots, z_n)$ such that $\alpha = z_n$.*

Proof. It follows from the definition of constructibility that α can be constructed from finitely many stages from the set $\{0, 1\} \subset \mathbb{Q}$. The result follows from this. □

Proposition 16. *Let E/F be a field extension with $[E : F] = n$, and let $\alpha \in E$. Then* $\deg(\alpha/F)$ *divides n.*

Proof. We know that $[F[\alpha] : F] = \deg(\alpha/F) = \deg(\text{minpoly}(\alpha/F))$. By the product of degrees formula, $[E : F] = [E : F[\alpha]] \cdot [F[\alpha] : F]$. The result follows. □

Proposition 17. *Let E be a constructed field. Then $[E : \mathbb{Q}]$ is a power of two.*

Proof. Since E is a constructed field, there exists a constructed tuple $(z_1, \dots, z_n)$, with $z_1 = i$, such that $E = \mathbb{Q}[z_1, \dots, z_n]$, with $z_{i+1} \in \mathbb{Q}[z_1, \dots, z_i]$.

Let $F_i = \mathbb{Q}[z_1, \dots, z_i]$ for $i = 1, \dots, n$; note $E = F_n$. We proceed by induction on n.

For $n = 1$, we have $z_1 = i$. Now $\operatorname{minpoly}(i/\mathbb{Q}) = X^2 + 1$, and $\deg(z_1/\mathbb{Q}) = 2$, so the proposition is true in this case.

Now suppose that $n > 1$, and let $F = F_{n-1}$ and $\alpha = z_n$. By induction, $[F : \mathbb{Q}]$ is a power of two. We also know that $i \in F$, so $z \in F$ if and only if $\Re z, \Im z, \overline{z}, |z|^2 \in F$.

Since α is constructible from F, it is the intersection of lines and circles given by points in F.

Case 1: α is the point of intersection of two lines given by F.
Note that the slope of a line through two points in F is also in F; let $y = m_1x+b_1$ and $y = m_2x + b_2$ be lines which intersect at α, where $m_1, b_1, m_2, b_2 \in F$. Then the point of intersection is the complex number $\alpha = \frac{b_2-b_1}{m_1-m_2} + \frac{m_1b_2-b_1m_2}{m_1-m_2} i$, whose real and imaginary parts are in F, so $\alpha \in F$ in this case, and $\deg(\alpha/F) = 1$.

Case 2: α is a point of intersection of a line and a circle given by F.
Let $y = mx + b$ and $(x - h)^2 + (y - k)^2 = r^2$ be the equations of the line and the circle. Now $m, b \in F$. Since $w = h + ki$ is the center of the circle, $h, k \in F$. Also there exists a point $z \in \mathbb{C}$ whose distance from w is r, so $r = |w - z| \in F$. Substitution gives $(x - h)^2 + (mx + b - k)^2 - r^2 = 0$; this is a quadratic equation whose solution is of the form $x = A+B\sqrt{D}$, where $A, B, D \in F$. Let $y = mx+b$; now $\alpha = x + yi$, and since $x, y \in F[\sqrt{D}]$, so is α.

Case 3: α is a point of intersection of two circles given by F.
Subtracting the equations of the circles cancels both the x^2 and the y^2 terms, producing a linear equation in x and y. Use this in combination with the equation of one of the circles to reduce to Case 2. □

Proposition 18. *Let $\alpha \in \mathbb{C}$ be constructible. Then there exist $p \in \mathbb{N}$ such that* $\deg(\operatorname{minpoly}(\alpha/\mathbb{Q})) = 2^p$.

Proof. If α is constructible, there exists a constructed tuple $(z_1, \dots, z_n)$ such that $\alpha = z_n$. Let $E = \mathbb{Q}[z_1, \dots, z_n]$; then $\alpha \in E$ and $[E : F]$ is a power of two. By a previous proposition, $\deg(\alpha/\mathbb{Q})$ divides $[E : F]$, so it is also a power of two. □

Proposition 19. *It is impossible to double a cube.*

Proof. Start with a cube whose sides have length one. To construct a cube with double the volume, one must be able to construct an edge of this cube; this requires the constructibility of the number $\alpha = \sqrt[3]{2}$.

The minimum polynomial of α over $\mathbb{Q}$ is $X^3 - 2$, so $\deg(\alpha/\mathbb{Q}) = 3$. Since 3 is not a power of 2, α is not constructible. □

Department of Mathematics and CSCI, Southern Arkansas University
E-mail address: `plbailey@saumag.edu`