3-1-1994

Extension fields.

Let E and F be fields. If F is a subfield of E, then E is an **extension field** of F. In this case, it's customary to write $F < E$. If $x \in E$ and $a \in F$, then the product $a \cdot x$ is defined in E. In this way, E becomes a vector space over F. Let $[E : F]$ denote the dimension of E over F — it is called the **degree** of E over F.

The dimension of a field over a subfield is a powerful tool. I'll use it to show the impossibility of certain ruler and compass constructions. The treatment here follows the excellent exposition of Irving Kaplansky [1].

Theorem. Suppose $K < F < E$. Then

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

(The statement is to be interpreted in the following way: If one side is finite, then both are, and they're equal.)

Proof. If $[E : K] < \infty$, then $[F : K] < \infty$ because F is a K-subspace of E. In addition, a basis for E over K clearly spans E over F, so $[E : F] < \infty$ as well.

Next, suppose that $[E : F] = m < \infty$ and $[F : K] = n < \infty$. I'll show that $[E : K]$ is finite, and that $[E : K] = mn$.

Suppose $\{x_1, \ldots, x_m\}$ is a basis for E over F, and $\{y_1, \ldots, y_n\}$ is a basis for F over K. I claim that $\{x_i y_j\}_{i,j}$ is a basis for E over K.

First, I'll show it spans. Let $z\ inE$. Since $\{x_1, \ldots, x_m\}$ is a basis for E over F,

$$z = \sum_i a_i x_i, \qquad a_i \in F.$$

Since $\{y_1, \ldots, y_n\}$ is a basis for F over K,

$$a_i = \sum_j b_{ij} y_j, \qquad b_{ij} \in K.$$

Then

$$z = \sum_i \left(\sum_j b_{ij} y_j\right) x_i = \sum_i \sum_j b_{ij}(x_i y_j).$$

This proves that $\{x_i y_j\}_{i,j}$ spans E over K.

Next, I'll show that $\{x_i y_j\}_{i,j}$ is indepedent over K. Suppose

$$\sum_i \sum_j b_{ij}(x_i y_j) = 0, \qquad b_{ij} \in K.$$

Then

$$\sum_i \left(\sum_j b_{ij} y_j\right) x_i = 0.$$

Now each term $\sum_j b_{ij} y_j$ is in F, because the y's are in F and the b's are in K. Since $\{x_i\}$ is independent over F,

$$\sum_j b_{ij} y_j = 0 \quad \text{for all } i.$$

By independence of the y's, $b_{ij} = 0$ for all i and j. This proves that $\{x_i y_j\}_{i,j}$ is independent. Hence, it's a basis for E over K. Since $\{x_i y_j\}_{i,j}$ has mn elements, $[E : K] = mn$, which is what I wanted to show. □

If $F < E$ and $u \in E$, $F(u)$ denotes the smallest subfield of E containing F and u. As usual, you can construct it by intersecting all subfields of E containing E and u.

There are two cases. Either u is a root of a polynomial with coefficients in F, or it is not. In the first case, u is **algebraic** over F; in the second case, u is **transcendental**.

Example. $\mathbb{Q} < \mathbb{R}$, $\sqrt{2} \in \mathbb{R}$, gives the subfield $\mathbb{Q}(\sqrt{2})$. This looks like all "rational functions" in $\sqrt{2}$ with $\mathbb{Q}$ coefficients; by rationalizing denominators,

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

$\sqrt{2}$ is algebraic over $\mathbb{Q}$, since it's a root of $x^2 - 2$. On the other hand, π is transcendental over $\mathbb{Q}$; π is not the root of any rational polynomial. (π *is* algebraic over $\mathbb{R}$, since it's a root of $x - \pi$.)

It is not so easy to prove that π is transcendental. Lindemann gave the first proof in 1882. □

Definition. A **monic polynomial** is a polynomial whose leading coefficient is 1.

If $f(x) = \sum_n a_n x^n$ is a polynomial, $a_m \neq 0$, and $a_n = 0$ for $n > m$, then a_m is the **leading coefficient** of $f(x)$.

Theorem. Let $F < E$, $u \in E$, u algebraic over F. Let $f(x)$ be a monic polynomial of smallest degree such that $f(u) = 0$, and let $\deg f = n$.

(a) f is unique.

(b) f is irreducible.

(c) $\{1, u, \ldots, u^{n-1}\}$ is a basis for $F(u)$ over F.

(d) $[F(u) : F] = n$.

(e) If g is a polynomial, then $g(u) = 0$ if and only if $f \mid g$.

Proof. (a) If

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \text{ and } g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

are both monic of minimal degree and both kill u, then

$$f(x) - g(x) = (a_{n-1} - b_{n-1})x^{n-1} + \cdots + (a_1 - b_1)x + (a_0 - b_0)$$

has smaller degree and also kills u. If any coefficient $a_i - b_i$ is nonzero, I may divide by the largest such, producing a monic polynomial which kills u and having degree less than the minimal degree $\times$. Hence, $f(x) - g(x) = 0$, and $f = g$.

(b) Suppose $f(x) = g(x)h(x)$, $\deg g, \deg h < \deg f$. Then $0 = f(u) = g(u)h(u)$. One of $g(u)$, $h(u)$ must be 0, and by dividing by the leading coefficient I obtain a monic polynomial killing u and having degree less than the degree of f $\times$. Hence, there is no such factorization, and f is irreducible.

(c) Suppose

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Then

$$0 = u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0,$$

$$u^n = -a_{n-1}u^{n-1} - \cdots - a_1 u - a_0.$$

Inductively, I may write u^{n+1}, u^{n+2}, …in terms of 1, u, …, u^{n-1}.

Now let K be the F-subspace of E spanned by 1, u, …, u^{n-1}, i.e. all expressions $a_0 + a_1 u + \cdots + a_{n-1}u^{n-1}$. The preceding argument shows that K contains all polynomials in u. It's then clear that K is closed under addition and multiplication, so it's a subring of E; I will show that K is a field. I only need to show that nonzero elements are invertible *in* K (I know they're invertible in E).

Suppose $g(u) = a_0 + a_1 u + \cdots + a_{n-1}u^{n-1} \neq 0$. f is irreducible, and $g(x)$ has degree less than $n = \deg f$, so f and g are relatively prime. Therefore, there are polynomials $a(x)$, $b(x)$, such that

$$a(x)f(x) + b(x)g(x) = 1.$$

Plug in u:

$$a(u) \cdot 0 + b(u)g(u) = 1, \quad b(u)g(u) = 1.$$

$b(u) \in K$ is the inverse of $g(u)$. Hence, K is a field.

Now on the one hand, K is a field containing F and u. On the other hand, any field containing F and u must contain all expressions of the form $a_0 + a_1 u + \cdots + a_{n-1}u^{n-1}$, i.e. must contain K. It follows that $K = F(u)$.

Thus, I've shown that $\{1, u, \ldots, u^{n-1}\}$ spans $F(u)$ over F. To see that $\{1, u, \ldots, u^{n-1}\}$ is independent, note that if

$$a_0 + a_1 u + \cdots + a_{n-1}u^{n-1} = 0,$$

then all the a's must be 0. For if not, $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ is a polynomial killing u of degree less than $\deg f$, and I get a monic polynomial killing u of degree less than $\deg f$ by dividing by the leading coefficient $\times$.

Therefore, $\{1, u, \ldots, u^{n-1}\}$ is a basis for $F(u)$ over F.

(d) This is trivial, given (c).

(e) Suppose $g(x) \in F[x]$ and $g(u) = 0$. Write

$$g(x) = f(x)q(x) + r(x) \quad \text{where} \quad \deg r < \deg f.$$

Then

$$0 = g(u) = 0 \cdot q(u) + r(u) = r(u).$$

If $r(x) \neq 0$, then dividing r by its leading coefficient produces a monic polynomial killing u of degree less than $\deg f$ $\times$. Hence, $r(x) = 0$, and $f \mid g$. □

Definition. Let $F < E$, $u \in E$, u algebraic over F. Let $f(x)$ be the monic polynomial of smallest degree such that $f(u) = 0$. f is called the **minimal polynomial** of u over F; it is sometimes denoted $\operatorname{irr}(u, F)$. The degree of $\operatorname{irr}(u, F)$ is called the **degree** of u over F.

Corollary. If F is a field and $f(x) \in F[x]$, there is an extension E of F in which $f(x)$ has a root.

Proof. Let $g(x)$ be an irreducible factor of $f(x)$. Then $\langle g(x) \rangle$ is maximal, so $F[x]/\langle g(x) \rangle$ is a field.

The map $\phi : F \to F[x]/\langle g(x) \rangle$ by

$$\phi(a) = a + \langle g(x) \rangle$$

is easily checked to be a ring map. To see that it's injective, suppose $\phi(a) = \langle g(x) \rangle$. Then $a \in \langle g(x) \rangle$, so $g(x) \mid a$. g is irreducible, so it's not a unit, and hence not a nonzero constant. By examining degrees, this divisibility relationship is impossible unless $a = 0$. Therefore, $\ker \phi = \{0\}$, so ϕ is injective. It follows that F embeds as a subfield of $F[x]/\langle g(x) \rangle$, and I can regard it as a *subset* by identifying it with its image.

Finally,

$$g\left(x + \langle g(x) \rangle\right) = g(x) + \langle g(x) \rangle = \langle g(x) \rangle.$$

That is, $x + \langle g(x) \rangle$ is a root of $g(x)$ in the field $F[x]/\langle g(x) \rangle$. Therefore, it's also a root of $f(x)$. □

Example. Applying the Corollary to $x^2+1 \in \mathbb{R}[x]$ produces the field $\mathbb{R}[x]/\langle x^2+1\rangle$, in which x^2+1 has the root $x+\langle x^2+1\rangle$. Of course, $\mathbb{R}[x]/\langle x^2+1\rangle \approx \mathbb{C}$ — this is an algebraic way of constructing the complex numbers from the reals. □

Example. (Ruler and compass constructions) Start with points in the plane with integer coordinates:

$$\{(m,n) \mid m,n \in \mathbb{Z}\}.$$

This corresponds to the idea that you can take a compass and randomly mark a length on a line, using that length to serve as a unit of measurement.

I'll adjoin points in the plane to this set by intersecting lines and circles. I'll say a point is **contructible** if it comes from the original set by a finite sequence of such additions. A number $u \in \mathbb{R}$ is **constructible** if $(u,0)$ is constructible.

Here are the ways I'm allowed to adjoin points:

1. If A, B, C, D are previously constructed points, I may add the point of intersection of the lines AB and CD.

2. If A, B, C, D are previously constructed points, I may add the point(s) of intersection of the line AB with the circle having center C and radius CD.

3. If A, B, C, D are previously constructed points, I may add the point(s) of intersection of the circles with centers A and C and radii AB and CD.

It's easy to see that rational numbers may be constructed in this way. Essentially, I start with the field $\mathbb{Q}$ as my set of constructible numbers. As I throw in points, I'm extending $\mathbb{Q}$ by subfields of $\mathbb{R}$:

$$\mathbb{Q} < F_1 < F_2 < \cdots.$$

Think about the equations of lines and circles. Lines are linear equations, circles are quadratic. All the coefficients are constructible numbers. When I intersect these lines and circles, the intersection points are roots of quadratics. *I'm always adding points whose coordinates are roots of quadratics.* This means that at each stage, a field extension has the form $F_n < F_n(\sqrt{u})$, $u \in F$. But the minimal polynomial of u over F is $x^2 - u$, so $[F(\sqrt{u}) : F] = 2$.

Conclusion: A number $u \in \mathbb{R}$ is constructible if it lies in an extension in a finite tower

$$\mathbb{Q} < \mathbb{Q}(\sqrt{a_1}) < \cdots < \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n}).$$

Since each step has degree 2, the whole thing has degree 2^n. Thus, u must be algebraic over $\mathbb{Q}$ of degree 2^n for some n.

Now consider some of the classical ruler and compass constructions.

Squaring the circle means constructing a square with the same area as a given circle. Taking the circle to have radius 1, I see that I need a square of side $\sqrt{\pi}$. π isn't even algebraic, so this is clearly impossible.

Duplicating the cube means to construct from (the side of) a given cube (the side of) a cube having twice the volume. If the given cube has side 1, the doubled cube must have side $\sqrt[3]{2}$. But the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$, which has degree 3. $3 \neq 2^n$, so this is impossible.

Finally, **trisecting an angle** requires the trisection of an arbitrary angle; I'll show that 60° can't be trisected. It suffices to show that $2\cos 20^\circ$ can't be constructed (i.e. you can't construct a 20° angle).

Use the trig identity

$$\cos 3\theta = 4(\cos\theta)^3 - 3\cos\theta.$$

Take $\theta = \cos 20^\circ$; this becomes

$$(2\cos 20^\circ)^3 - 3(2\cos 20^\circ) - 1 = 0.$$

The polynomial $x^3 - 3x - 1$ is irreducible over $\mathbb{Q}$ of degree 3, so it must be the minimal polynomial of $2\cos 20°$. Hence, $2\cos 20°$ has degree 3, and can't be contructed. $\square$

---

[1] Irving Kaplansky, *Fields and rings.* Chicago: The University of Chicago Press, 1972.

