Summary, April 16

FIELDS

When $F \subset K$ are two fields, one contained in the other, K is called a *field extension* of F.

Let K be an extension of F. It becomes an F-vector space, scalar multiplication by an element of F being multiplication in K. The dimension of that space is called the *degree* of K over F, and is denoted by

$$[K : F] = \dim {}_F K$$

For example, the field of complex numbers is an extension of the real numbers, and its degree $[\mathbb{C} : \mathbb{R}]$ is 2.

Let $F \subset K$ be a field extension, and let α be an element of K. We can map the ring $F[x]$ of polynomials with coefficients in F to K:

$$F[x] \xrightarrow{\varphi} K$$

by sending F to itself by the identity map and substituting α for the variable x: $\varphi(f(x)) = f(\alpha)$. The image of this map will be denoted by $F[\alpha]$. It is the set of elements β of K that have the form $\beta = f(\alpha)$ for some polynomial $f(x)$.

The kernel I of φ is the set of polynomials f such that $f(\alpha) = 0$, i.e., such that α is a root of f in K. It is a principal ideal, as are all ideals of $F[x]$. The element α is *algebraic over* F if the kernel I is not the zero ideal. Let's assume that α is algebraic over F, and let

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

be a monic polynomial that generates the kernel I.

Lemma 1. The monic polynomial $f(x)$ that generates the kernel I has these properties:

- α is a root of f,
- $f(x)$ is an irreducible element of $F[x]$.
- $f(x)$ is the unique monic irreducible polynomial with coefficients in F with root α.

proof The first assertion is obvious. For the second, we note that if $f(x) = g(x)h(x)$ then $f(\alpha) = g(\alpha)h(\alpha)$, so if $f(\alpha) = 0$, then either $g(\alpha)$ or $h(\alpha) = 0$. When g an h have positive degree, that degree is less than the degree d of F. Neither one can be in the principal ideal I that f generates, so they can't have α as a root. (Of course, $f(x)$ isn't an irreducible element of $K[x]$ because it has a root α in K.)

For the third assertion, if $g(x)$ is a monic polynomial in $F[x]$ that has root α, then f divides g, so g won't be irreducible unless $f = g$. □

Corollary. Let $F \subset K$ be a field extension, and let α be an element of K that is algebraic over F.
(i) The kernel $I = (f)$ of the map φ is a maximal ideal.
(ii) The image $F[\alpha]$ of the substitution map φ is isomorphic to the quotient ring $F[x]/(f)$.
(iii) The image $F[\alpha]$ is a field.
(iv) If d is the degree of the irreducible polynomial for α, then the elements $(1, \alpha, \alpha^2, ..., \alpha^{d-1})$ form a basis for $F[\alpha]$.

proof (i) If I is contained in another ideal J, then that ideal is a principal ideal, say generated by the monic polynomial g. Then g divides f, and since f is irreducible, $g = f$ or else $g = 1$.

(ii) The First Isomorphism Theorem tells us that the image $F[\alpha]$ is isomorphic to the quotient ring $F[x]/I$.

(iii) Because I is a maximal ideal, the quotient ring is a field.

(iv) This is true because, in the isomorphic quotient ring $F[x]/(f)$, the residues of the elements $(1, x, x^2, ..., x^{d-1})$ for a basis. □

Example. Let F be the field $\mathbb{Q}$ of rational numbers, and let α be the cube root of 2. The irreducible polynomial for α over F is of course $x^3 - 2$. Why is $F[\alpha]$ a field? In particular, how can we invert a nonzero element such as $\beta = 1 + \alpha$ in $F[\alpha]$? The reason is that, because f is irreducible, multiplication by β will be an injective

linear operator $F[\alpha] \to F[\alpha]$. When we write nonzero elements β, γ as polynomials in α of degrees $< d$, we see that $\beta\gamma \neq 0$. Then multiplication by β is surjective because $F[\alpha]$ is a finite dimensional F-vector space.

To be explicit with $\beta = 1 + \alpha$ and $\alpha^3 = 2$, we look for an element γ such that $\beta\gamma = 0$. This element will be a combination of $1, \alpha, \alpha^2$. We have

$1(1 + \alpha) = 1 + \alpha$
$\alpha(1 + \alpha) = \alpha + \alpha^2$
$\alpha^2(1 + \alpha) = 2 + \alpha^2$.

Then $(\alpha^2 - \alpha + 1)(1 + \alpha) = 3$. So $(1 + \alpha)^{-1} = (\alpha^2 - \alpha + 1)/3$.

There is just one important fact about the degree $[K : F]$ of a field extension, its multiplicative property:

Theorem. Let $F \subset K \subset L$ be fields. Then $[L : F] = [L : K][K : F]$.

proof This is really very simple. Let $(\beta_1, ..., \beta_n)$ be a basis for L as K-vector space, and let $(\alpha_i, ..., \alpha_m)$ be a basis for K as F-vector space. So $[L : K] = n$ and $[K : F] = m$. We show that the set of mn products $\{\alpha_i\beta_j\}$ is a basis fr L as F-vector space.

Let γ be an element of L. We write γ as a combination $\sum_j b_j\beta_j$ of the K-basis $(\beta_!, ..., \beta_n)$, with b_j in K, and we write each element b_j of K as a combination $b_j = \sum_i a_{ij}\alpha_i$ of the F-basis $(\alpha_1, ..., \alpha_m)$ of K. Substituting for b_j,

$$\gamma = \big(\sum_i a_{ij}\alpha_i\big)\beta_j = \sum_{i,j} a_{ij}\alpha_i\beta_j$$

So the products $\alpha_i\beta_j$ span L. The coeffiients b_j are unique, and so are the coefficients a_{ij}. Therefore the elements $\{\alpha_i\beta_j\}$ are independent. □

Corollary. Let $F \subset K$ be a field extension and let α be an element of K of degree d over F. Then d divides the degree $[K : F]$ of the field extension.

Sample application: Let F be the field of rational numbers, and let α be a cube root of 2. Then α isn't an element of the extension $K = F[\sqrt{2}, \sqrt{3}, \sqrt{5}]$. The reason is that we can obtain K from F in three steps, adjoining the square roots one at a time. Each square root adjunction gives us a field extension of degree (at most) 2, so $[K : F]$ divides 8. (It is equal to 8.) Then α, which has degree 3 over F, isn't in K.

trisection of an angle

This is a more interesting application of the theorem.

The problem is this: An angle η is formed by two intersecting lines in the plane, and the problem is to construct two lines meeting in an angle $\theta = \frac{1}{3}\eta$. This isn't always possible using ruler and compass. One cannot trisect the angle 60° though some angles, for instance 90°, can be trisected.

To prove that one cannot trisect 60°, we must be precise about what constructions are allowed.

The rules for ruler and compass construction are as follows:

• Two points in the plane are given. They are considered to be constructed.

• One may construct a line through two constructed points, and one may construct a circle whose center is at one constructed point and that passes through another constructed point.

• intersections of lines and circles that have been constructed are constructed points.

That is all. One isn't allowed to use the ruler for measuring, and one isn't allowed to choose an "arbitrary" point.

The two points define a unit length. To start, one constructs the line through the two given points. That line becomes the x-axis, one point is the origin $(0, 0)$ and the other is the point $(1, 0)$.

Then we can construct two circles, the unit circle centered at the origin and the one centered at the point $(1, 0)$. These two circles and the line provide us with four more constructed points, their intersections, which are the points $(-1, 0), (0, 2)$, and $\frac{1}{2}(1 \pm \sqrt{3}, 1)$. At this point, there are too many possible constructions to list.

Using allowed constructions, one can copy the two lines meeting in the angle η to any desired position in the plane. Let's not take the time to probve this. It is proved in the text.

So we may suppose that the intersection of the lines defining η is the origin, and that one of the lines is the x-axis. Then the problem becomes to construct the line ℓ that makes an angle $\theta = \eta/3$ with the x-axis. The intersection of ℓ with the unit circle has coordinates $\cos\theta, \sin\theta$. If we can construct θ, we will also be able to construct its cosine as a length on the x-axis, and its cosine is the root of a cubic equation. It is easy to compute this cubic equation when one writes the cosine in terms of the exponential function. Let $\alpha = 2\cos\theta = e^{i\theta} + e^{-i\theta}$. Then

$$\alpha^3 = (e^{3i\theta} + e^{-3i\theta}) + (e^{i\theta} + e^{-i\theta}) = 2\cos\eta + \alpha$$

So if we write $\beta = 2\cos\eta$, then $\alpha^3 - \alpha - \beta = 0$, and α is a root of the cubic polynomial $x^3 - x - \beta$.

If $\eta = 60^\circ$, then $\beta = 1$, $\theta = 20^\circ$, so $\alpha = 2\cos\theta$ is a root of the polynomial $x^3 - x - 1$, which is irreducible over the field $F = \mathbb{Q}$ of rational numbers. The degree of $\cos\theta$ over the rational numbers is three. We'll use this fact to show that The angle 20° cannot be constructed by ruler and compass.

Proposition. Let X and Y be two lines, a line and a circle, or two circles that have been constructed using constructed points whose coordinates are in a field extension K of F. Then the coordinates of the intersection points are either in K, or in a quadratic extension of K.

Corollary. It is impossible to construct a pair of lines meeting in an angle of 20°.

proof of the corollary By induction, the field generated by the coordinates of a finite set of contructed points will be obtained by a succession of quadratic extensions from the field of rational numbers F. Its degree over F will be a power of 2, while $\cos 20^\circ$ has degree 3 over F. □

proof of the proposition We'll use the equations of the form $ax + by + c = 0$ and $(x-p)^2 + (y-q)^2 = r^2$ to describe lines and circles.

The intersection of two lines is found by solving a system of linear equations, so the coordinates will be in K. To find the intersection of a line $ax + by + c = 0$ with a circle $(x-p)^2 + (y-q)^2 = r^2$, we solve the linear equation for $y = -(ax - c)/b$ and substitute into the equation of the circle, obtaining a quadratic equation in x. If a, b, c, p, q, r are in K, the solutions will be in K or in a quadratic extension of K. Finally, if two circles have equations $(x - p_1)^2 + (y - q_1)^2 = r_1^2$ and $(x - p_2)^2 + (y - q_2)^2 = r_2^2$, the common solutions can be obtained in this way: The difference of the two equations is the linear equation

$$2(p_2 - p_1)x + 2(q_2 - q_1)y = -(p_1^2 - p_2^2) + (r_1^2 - r_2^2)$$

The common solutions can also be obtained by solving the pair consisting of this linear equation and one of the quadratic equations. This puts us back in the case of a circle and a line. (The line is the one joining the two points of intersection.) □