FEBRUARY 8 NOTES

1. 13.2: Algebraic Extensions

From last time:

Definition 1.1. Let F be a field and let K be an extension of F. An element $\alpha \in K$ is **algebraic** over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F, we say that α is **transcendental** over F. The extension K/F is **algebraic** if every element of K is algebraic over F.

Remark 1.2. If α is algebraic over F, then it is algebraic over any extension L of F (because algebraicity over F implies it is a root of a polynomial in $F[x]$, and $F \subset L$, so it is a root of a polynomial in $L[x]$).

Proposition 1.3. *Let α be algebraic over F. Then, there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. A polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$.*

This polynomial is called the ***minimal polynomial*** *for α over F. If F is clear from context, it is denoted simply by $m_\alpha(x)$. The* ***degree*** *of α is defined to be the degree of $m_\alpha(x)$.*

We ended last time proving a theorem that implies:

Corollary 1.4. If K/F is finite, then it is algebraic.

Example 1.5. Let F be a field of characteristic not equal to 2 and let K/F be any extension with $[K : F] = 2$. Then, for any $\alpha \in K$ with $\alpha \notin F$, $\deg m_\alpha(x) \leq 2$. It cannot be 1 because $\alpha \notin F$. Therefore, the minimal polynomial of α is $m_\alpha(x) = x^2 + bx + c$ for some $b, c \in F$. Also, since $F \subset F(\alpha) \subset K$ and $F(\alpha)$ and K are both two dimensional vector spaces over F, we have $K = F(\alpha)$.

We can determine all possible elements in K by the quadratic formula: we find that

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

where the symbol $\sqrt{b^2 - 4c}$ denotes the root of the equation $x^2 - (b^2 - 4c) = 0$. Let $\sqrt{D} = \sqrt{b^2 - 4c}$. Because $\alpha \in F(\sqrt{D})$ by definition and we can similarly show $\sqrt{D} \in F(\alpha)$, we have $F(\alpha) = F(\sqrt{D})$.

Therefore, **every** degree 2 extension K of F is of the form $F(\sqrt{D})$ where $D \in F$ is not a square. These extensions are called **quadratic extensions** of F.

A few more generalities on field extensions:

Theorem 1.6. *Let $F \subset K \subset L$ be fields. Then, $[L : F] = [L : K][K : F]$.*

Proof. Suppose first that $[L : K] = m$ and $[K : F] = n$. If $\{\alpha_i\}$ is a basis for L/K and $\{\beta_j\}$ is a basis for K/F, then every element of L can be written as $\sum a_i\alpha_i$ for some $a_i \in K$, but every $a_i \in K$ can be written as $\sum b_{ij}\beta_j$, so every element in L can be written as $\sum b_{ij}\alpha_i\beta_j$, i.e. the elements $\alpha_i\beta_j$ span the vector space L over F. It suffices to show that they are linearly independent. If there is a linear combination $\sum b_{ij}\alpha_i\beta_j = 0$, then following the process in reserve and defining $a_i = \sum b_{ij}\beta_j$, we find that $\sum a_i\alpha_i = 0$, which implies that each $a_i = 0$. This implies that $0 = a_i = \sum b_{ij}\beta_j$, so we conclude $b_{ij} = 0$ for all i, j and hence the elements $\alpha_i\beta_j$ are linearly independent. This basis has mn elements, so we conclude that $[L : F] = [L : K][K : F]$.

Now, suppose something in the desired expression is infinite. Note that the previous paragraph shows that, if $[L : K]$ and $[K : F]$ are both finite, then $[L : F]$ is finite, so if $[L : F]$ is infinite, either $[L : K]$ or $[K : F]$ is infinite. If $[K : F]$ is infinite, as $K \subset L$, we must have $[L : F]$ infinite. Similarly, if $[L : K]$ is infinite, then $[L : F]$ is infinite. Therefore, if one side of the equation is infinite, so is the other. $\square$

Corollary 1.7. If L/F is finite and $F \subset K \subset L$, then $[K : F]$ divides $[L : F]$.

This allows us to prove *specific things about numbers*!

Example 1.8. The element $\sqrt{2}$ cannot be contained in any field $\mathbb{Q}(\alpha)$ where $\mathbb{Q}(\alpha)/\mathbb{Q}$ has degree 3, because 2 does not divide 3. Therefore, if α is any root of an irreducible degree 3 polynomial over $\mathbb{Q}$, we cannot write $\sqrt{2}$ as a rational linear combination of $1, \alpha, \alpha^2$.

Example 1.9. Because $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$ and $(\sqrt[6]{2})^3 = \sqrt{2}$, we have $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[6]{2})$, and by multiplicativity of degrees, $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$. Therefore, the minimal polynomial of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$ has degree 3. Because $x^3 - \sqrt{2}$ is a monic polynomial of degree 3 over $\mathbb{Q}(\sqrt{2})$ with $\sqrt[6]{2}$ as a root, it must be the minimal polynomial and hence must be irreducible over $\mathbb{Q}(\sqrt{2})$.

Definition 1.10. An extension K/F is finitely generated if there exist $\{\alpha_1, \dots, \alpha_n\} \in K$ such that $K = F(\alpha_1, \dots, \alpha_n)$.

We can compute these field extensions 'recursively', i.e.

Lemma 1.11. $F(\alpha, \beta) = (F(\alpha))(\beta)$.

Proof. This follows directly from minimality in the definition of these extensions. Because $F(\alpha, \beta)$ contains F and α, it contains $F(\alpha)$, and because it contains $F(\alpha)$ and β, it must contain $(F(\alpha))(\beta)$. Conversely, $(F(\alpha))(\beta)$ contains F and α and β so must contain $F(\alpha, \beta)$. Therefore, they are equal. $\square$

This tells us that $K = F(\alpha_1, \dots, \alpha_n)$ can be constructed iteratively by first letting $F_1 = F(\alpha_1)$ be the field generated by α_1 over F, and then $F_2 = F_1(\alpha_2)$ the field generated by α_2 over F_1 (which may be different than that over F!), etc to get a sequence

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

and supposing that α_i is algebraic over F of degree d_i, then α_i is algebraic over F_i of degree at most d_i, so we obtain that

$$[K : F] = [F_n : F_{n-1}] \dots [F_2 : F_1][F_1 : F_0] \le d_1 \dots d_n.$$

Example 1.12. The field $\mathbb{Q}(\sqrt[6]{2}, \sqrt{2})$ is just $\mathbb{Q}(\sqrt[6]{2})$ since $\sqrt{2}$ is already in $\mathbb{Q}(\sqrt[6]{2})$.

Example 1.13. The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is an extension of $\mathbb{Q}(\sqrt{2})$. We know the degree of the extension is at most 2 because $\sqrt{3}$ is a root of $x^2 - 3$, but we need to show that this still is irreducible over $\mathbb{Q}(\sqrt{2})$. This polynomial only has degree 2, so it is reducible if and only if it has a root in $\mathbb{Q}(\sqrt{2})$, which means $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. We can show this is impossible: if $\sqrt{3} = a + b\sqrt{2}$ for rational numbers a, b, then we get $3 = (a^2 + 2b^2) + 2ab\sqrt{2}$. If $ab \neq 0$, then we can solve for $\sqrt{2}$ to conclude that $\sqrt{2}$ is rational, a contradiction, so we must have $ab = 0$. If $b = 0$, then $\sqrt{3} = a$ is rational, a contradiction. If $a = 0$, then $\sqrt{3} = b\sqrt{2}$, which says $\sqrt{6} = 2b$, or $\sqrt{6}$ is rational, a contraction. Thus, $[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})]$ is 2, so $[\mathbb{Q}(\sqrt{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = 4$.

Using this, we can write a basis for $\mathbb{Q}(\sqrt{3}, \sqrt{2})$: we must have $1, \sqrt{2}, \sqrt{3}$, but then we must also have $\sqrt{2}\sqrt{3} = \sqrt{6}$ which is independent from the previous three, so these four elements are a basis.

Theorem 1.14. *The extension K/F is finite if and only if K is generated by a finite number of algebraic elements over F, and if these elements have degrees d_i, then $[K : F]$ has degree $\le \Pi d_i$.*

Proof. If K/F is finite of degree n, let $\alpha_1, \dots, \alpha_n$ be a basis for K over F. These are all algebraic because $[K : F]$ is finite and therefore K is generated by a finite number of algebraic elements over F. The converse and result on degree was proved above. $\square$

Corollary 1.15. Suppose α, β are algebraic over F. Then, $\alpha \pm \beta$, $\alpha\beta$, α/β (for $\beta \neq 0$) are algebraic over F.

Proof. These elements all lie in $F(\alpha, \beta)$ which is finite over F, hence they are algebraic. $\square$

Finally, note that we could extend these ideas slightly more generally:

Definition 1.16. Let $K_1, K_2 \subset K$ be fields. The **composite field** of K_1, K_2 is denoted K_1K_2 and is the smallest subfield of K containing both K_1 and K_2. (One can similarly define the composite field of any collection of subfields of K.)

By similar arguments to those above, one can show that

$$[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F] = [K_1K_2 : K_2][K_2 : F] \leq [K_1 : F][K_2 : F].$$

Note that this implies $[K_i : F]$ divides $[K_1K_2 : F]$, so for example, if $\gcd([K_1 : F], [K_2 : F]) = 1$, we have $[K_1K_2 : F] = [K_1 : F][K_2 : F]$.

2. 13.3: Straightedge and Compass Constructions

Finally, we say a few things about what angles and lengths and be constructed with just a straightedge and compass. Let us translate into algebraic terms: let 1 denote a fixed unit distance, so any length is $a \in \mathbb{R}$ a real number. We consider the usual xy-plane and view everything in this section in $\mathbb{R}^2$. We want to consider the problem of which lengths in $\mathbb{R}$ can be obtained from a compass and straightedge knowing just this unit distance. The lengths for which this is possible are the **constructible** real numbers.

We are allowed to:

(1) Draw a straight line connecting any two points.
(2) Mark a point of intersection of any two lines.
(3) Draw a circle with a given radius and center.
(4) Mark a point of intersection of lines and circles or multiple circles.

Exercise 2.1. Show that, given any line L, you can (1) draw a perpendicular line through any point of L, and then (2) draw any line parallel to L. (Hint for (1): draw several circles.)

From some geometry and similar triangles, we can construct several numbers:

Example 2.2. Suppose we are given two lengths a, b. Then, we may construct $a \pm b$, ab, a/b, and $\sqrt{a}$. We illustrate this pictorially (using that we can draw parallel and perpendicular lines):

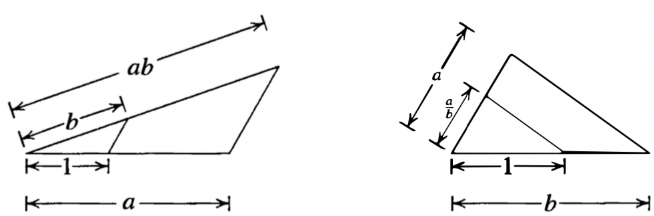

Fig. 1

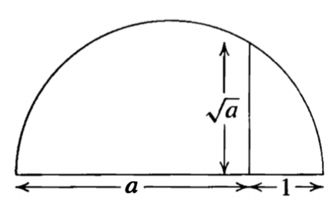

Fig. 2

How does this relate to field extensions?

Proposition 2.3. *If an element $\alpha \in \mathbb{R}$ is obtained from a field $F \subset \mathbb{R}$ by a series of compass and straightedge constructions, then $[F(\alpha) : F] = 2^k$ for some integer k.*

Before the proof, some examples of applications:

Example 2.4. Is it possible, using only a straightedge and compass, to construct a cube with precisely twice the volume of a given cube?

The answer is no! If so, we would need to start with a cube with side length 1 (so volume 1), and then construct a cube with volume 2, i.e. side length $\sqrt[3]{2}$. Because $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^k$, this is not possible.

Example 2.5. Starting with a given angle θ, is it possible to use only a compass and straightedge to trisect this angle?

The answer is no! If any given angle θ could be constructed, then we could determine the point at distance 1 from the origin along the line in angle θ, i.e. $\cos\theta$ (the x-coordinate) and $\sin\theta$ (the y-coordinate) can be constructed. Conversely, if we know $\cos\theta$ and $\sin\theta$, then we can construct the angle θ. So, trisecting the angle is equivalent to starting with $\cos\theta$ and finding $\cos\theta/3$. This is not always possible! There is a trig identity that says:

$$\cos\theta = 4\cos^3\theta/3 - 3\cos\theta/3$$

so if $\theta = 60$, then $\cos\theta = 1/2$, and letting $\beta = \cos 20$, we get

$$4\beta^3 - 3\beta - 1/2 = 0$$

or

$$8\beta^3 - 6\beta - 1 = 0.$$

Letting $\alpha = 2\beta$, this becomes $\alpha^3 - 3\alpha - 1 = 0$. This is an irreducible polynomial over $\mathbb{Q}$ (for instance, one could use the rational root theorem) so the extension $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ but this is again not a power of 2.

Now, let's prove the theorem:

Proof. Suppose we start with a field $F \subset \mathbb{R}$ of things we have constructed. (We know, from 1, we can construct all rational numbers, so the collection of elements that are constructible from 1 is some field larger than $\mathbb{Q}$ in $\mathbb{R}$.) A straight line connecting any two points with coordinates in F has equation of the form $ax + by - c = 0$ where $a, b, c \in F$. Solving two such equations (finding the intersection point) gives solutions in F, so using only a straightedge will just produce points in F.

Using a compass, supposing we have constructed the coordinates of the center (h, k) and the radius r, we have equation $(x-h)^2 + (y-k)^2 = r^2$ where $h, k, r \in F$.

We can compute the intersection point of lines with coordinates in F, i.e. $ax+by-c$, and solving for y and substituting into the equation of the circle, the x-coordinate of the point of intersection lies in (at worst) a quadratic extension of F, and hence so does y as it is linear in x. If we intersect two circles, $(x-h)^2+(y-k)^2 = r^2$ and $(x-h')^2+(y-k')^2 = r'^2$ we can subtract the first from the second to get the equations $(x-h)^2+(y-k)^2 = r^2$ and $2(h'-h)x+2(k'-k)y = r^2-h^2-k^2-r'^2+h'^2+k'^2$ which is just the intersection of a circle and line, so the coordinates lie in a quadratic extension of F. Therefore, if $\alpha \in \mathbb{R}$ is obtained from elements in F by a finite sequence of straightedge and compass operations, then α is an element of an extension field K/F with $[K : F] = 2^m$, and hence $[F(\alpha) : F] = 2^k$ for some $k \leq m$ because it is a divisor of 2^m. $\square$