Galois Theory

October 24, 2019

0 A Bit of History, Notation, and Revision

Historically the subject arose from looking at solutions to polynomial equations in one variable over $\mathbb{C}$. The question arose as to whether polynomials could be solved by a formula involving the coefficients and taking roots ("soluble by radicals"). From school, we know that we can solve quadratics in this way with $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$. For a long time it has been known that cubics and quartics have similar, albeit more complicated, formulae for their roots. This was studied by Lagrange in the 1770s. In 1799 Ruffini claimed that there was no general formula in the case of quintics, however there was a gap in his proof. It wasn't until Abel in 1824 that there was a complete accepted proof, using permutations of roots of polynomials. This was the start of group theory.

Galois gave the first explanation of when a quintic was was soluble by radicals or not in 1831, using the structure of a group of permutations of the roots, in particular the importance of normal subgroups. Galois' work was not known until Liouville published his papers in 1846. Liouville realised the connection with Cauchy's work on permutations, but didn't realise the importance of the group-theoretic structure, and in fact few of the contemporary mathematicians did so.

Galois entered his papers for various competitions and also for the entrance process for the École Polytechnique in Paris. He didn't get in however, and went to another university in Paris, where he got involved in politics and eventually killed in a duel. Before the duel he left a 6½ page manuscript setting out his ideas about the future development of the theory. His papers have been carefully studied by Peter Neumann:

The Mathematical Writings of Évariste Galois
History of European Mathematics
European Mathematical Society

This course is presented in a more modern fashion. Rather than thinking about roots of polynomial equations we think about field extensions. Recall from GRM, if K is a field, and f is an irreducible polynomial in $K[x]$, then $K[x]/f$ is also a field.[1]

Books

There is a historical introduction in I. Stewart's Galois Theory, which is very readable but doesn't quite cover the syllabus. Other books are Artin's Galois Theory; Van der Waerden's Modern Algebra; Lang's Algebra; and Kaplansky's Fields and Rings.

[1] Alternative notation is to use $K[x]/(f)$, where (f) is the ideal generated by f

Notation / Revision

In this course, a ***ring*** means a commutative ring with a **1**
A ***field*** means a ring in which all non-zero elements have multiplicative inverses, i.e. are units, e.g. $\mathbb{Q}, \mathbb{R}, \mathbb{Z}/\mathbb{Z}_p$ for p prime.
For a ring R, R^X is the set of units of R, so if K is a field, we have $K^X = K \setminus \{0\}$
$R[x]$ is the ring of polynomials with coefficients in R, with variable denoted by x[2].

UnderlineExercise: If R is an integral domain then $R[x]$ is an integral domain.

If K is a field then $K[x]$ is a Euclidean domain.
If $a, b \in K[x]$ then $\exists\, q, r$ such that $a = qb + r$ with $\deg r < \deg b, b \neq 0$

Corollary 0.1.

1. *$K[x]$ is a principal ideal domain (PID)*
2. *$K[x]$ is a unique factorisation domain (UFD)*
3. *For $f \in K[x]$, f irreducible $\iff$ f prime $\iff$ (f) is maximal $\iff$ $K[x]/(f)$ is a field*
4. *For $a, b \in K[x], (a) + (b)$ is an ideal and so is of the form (g) for some $g \in K[x]$. $g = \gcd(a, b)$, and is unique up to a unit.*
5. *If $f \in K[x] \setminus \{0\}$ then f has at most $\deg f$ roots in K.*[3]

Proof. Left as an exercise □

$K(x)$ is the ***fraction field*** of $K[x] \coloneqq \{$equivalence classes f/g where $f/g = r/s \iff fs = gr\}$

1 Field Extensions, Algebraic and Transcendental Numbers

1.1 Definitions

If $K \subseteq L$ is a subring that is also a field, the L is an ***extension*** of K. We write this extension as L/K.
e.g. $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $K[x]/K$, L/K where $L = K[x]/(f)$, f irreducible.
Observe that, if L/K is a field extension then L can be regarded as a vector space over K.

We then define $[L : K] = \dim_K L$, the dimension of the vector space of L over K, to be the ***degree*** of the field extension L/K. If $[L : K] < \infty$, then it is called a finite field extension, otherwise an infinite field extension.
e.g. $[\mathbb{C} : \mathbb{R}] = 2$, $\mathbb{R}-$basis is $\{1, \mathrm{i}\}$

A field K always has a smallest subfield. There is a ring homomorphism $\mathbb{Z} \to K; 1 \mapsto 1$. Either this is injective, in which case we get $\mathbb{Q} \subseteq K$, and the ***characteristic*** of K is 0, written $\operatorname{char} K = 0$, or it is not injective, in which case $1 + 1 + \ldots + 1 = 0$ for some prime number of 1s p, and we get $\mathbb{F}_p \subseteq K$, and the ***characteristic*** of K is p. E.g. $\operatorname{char} \mathbb{F}_p(x) = p$, as $p \cdot 1 = 0$ in $\mathbb{F}_p \subseteq \mathbb{F}_p(x)$.

[2] $= \left\{\sum_{i \geq 0} r_i x^i\right\}$ where all but finitely many r_i are non-zero
[3] We say α is a root of $f \iff f(\alpha) = 0$

K is a ***finite field*** if $\#K < \infty$, where $\#K$ denotes the number of elements of K.

Lemma 1.1. *If F is a finite field then* $\operatorname{char} F = p$ *for some prime p, and $\#F = p^n$ for some $n \geq 1$.*

Proof. If $\#F < \infty$ then the map $\mathbb{Z} \to F$ is not injective, so $\mathbb{F}_p \subseteq F$ and F is a finite dimensional vector space over $\mathbb{F}_p$, and hence as a $\mathbb{F}_p$-vector pace $F \cong \mathbb{F}_p^n$, and hence has p^n elements. □

We'll see later that in fact there is a unique field of p^n elements for each prime p and integer $n \geq 1$

Given a field extension L/K and some $\alpha \in L$, we define $K[\alpha]$ to be the smallest subring of L containing K and α, and $K(\alpha)$ to be the smallest such subfield. As such, $K[\alpha] = \{\sum_{i=1}^{N} r_i \alpha : r_i \in K, N \in \mathbb{N}\}$, whilst $K(\alpha) = \{f/g : f, g \in K[\alpha], g \neq 0\}$.

E.g.: $\mathbb{Q}[\mathfrak{i}] = \{a_0 + a_1\mathfrak{i} + a_2\mathfrak{i}^2 + \ldots + a_n\mathfrak{i}^n : a_i \in \mathbb{Q}\} = \{a_0 + a_1\mathfrak{i} : a_0, a_1 \in \mathbb{Q}\}$. This is already a field, so $\mathbb{Q}(\mathfrak{i}) = \mathbb{Q}[\mathfrak{i}]$.

NOTE: If x an indeterminate then we can define a ring homomorphism $\phi : K[x] \to L; x \mapsto \alpha$, and $K[\alpha] = \operatorname{im} \phi$.

α is ***transcendental*** over K if ϕ is injective. α is ***algebraic*** over K if ϕ is not injective. If ϕ is not injective, then $\ker \phi$ is a non-zero ideal, hence $\ker \phi = (f)$ for some $f \in K[x]$ with $f(\alpha) = 0$. If ϕ is injective, then the preimage of 0 is exactly $\{0\}$, and so there is no polynomial over K with root α. Hence α algebraic over K if and only if there is some polynomial over K with root α.

If $\ker \phi = (f)$, then f is the polynomial of least degree such that $f(\alpha) = 0$. Sometimes we also require f to be monic, and call it the ***minimal polynomial*** of α over K. We also define the ***degree*** of α over K as $\deg_K \alpha = \deg f$.

f is irreducible - if $f = gh$, then $f(\alpha) = g(\alpha)h(\alpha) = 0$, but L is an integral domain so one of g, h is a smaller polynomial with a zero at α ↯. As such, f has non-zero constant term,

$$\alpha^{-1} = \frac{1}{a_0}\left(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a^1\right)$$

Proposition 1.2. *α is transcendental over K if and only if $\phi : K[x] \to K[\alpha]$ an isomorphism which extends to an isomorphism $K(x) \to K(\alpha)$. In particular, all transcendental extensions $K(\alpha)$ are mutually isomorphic, being isomorphic to $K(x)$.*

To summarise:

Proposition 1.3. *Given a field extension L/K and $\alpha \in L$, the following are all equivalent:*

1. *α is algebraic over K*
2. *$[K(\alpha) : K] < \infty$*
3. *$\dim_K K(\alpha) < \infty$*
4. *$K[\alpha] = K(\alpha)$*
5. *$K[\alpha]$ is a field*

When these hold, $[K(\alpha) : K] = \deg_K \alpha$

Proof. Let $d = \deg_K \alpha = \deg f$, where f is the minimal polynomial of α over K. Observe $1, \alpha, \alpha^2, \ldots, \alpha^d$ span $K(\alpha)$, and the minimality of the degree of f imply that $1, \alpha, \ldots, \alpha^{d-1}$ are linearly independent. □

Warnings

1. "Algebraic" and "transcendental" depend on K - e.g. $2\pi\mathfrak{i} \in \mathbb{C}$ is algebraic over $\mathbb{R}$ with minimal polynomial $x^2 = -4\pi^2$, but is transcendental over $\mathbb{Q}$.
2. The minimal polynomial is dependent on K - e.g. $\alpha = \sqrt{\mathfrak{i}} = (1+\mathfrak{i})\frac{\sqrt{2}}{2}$. The minimal polynomial of α over $\mathbb{Q}$ is $x^4 + 1$, whilst over $\mathbb{Q}(\mathfrak{i})$ it is $x^2 - \mathfrak{i}$. Note that in this example $[\mathbb{Q}(\mathfrak{i}) : \mathbb{Q}] = 2; [\mathbb{Q}(\alpha) : \mathbb{Q}(\mathfrak{i})] = 2; [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, and $2 \times 2 = 4$, illustrating the ***tower law***.

Theorem 1.4 (Tower Law)**.** *Given field extensions $M/L/K$, then M/L is finite if and only if M/K and L/K are finite. In that case, $[M : K] = [M : L][L : K]$.*

This can be deduced from the following proposition:

Proposition 1.5. *Suppose L/K is a finite field extension, and V is a vector space over L. Then V is finite dimensional over L if and only if V is finite dimensional over K and* $\dim_K V = \dim_L V \times [L : K]$

Proof that Prop. 1.5 $\implies$ the tower law. If L/K is not finite then M/K is not a finite extension. Otherwise, apply **1.5** with $V = M$. □

Proof of Prop. 1.5. If $\dim_L V = d$, take a L-vector space basis of V, say $\{\alpha_1, \ldots, \alpha_d\}$, and K-vector space basis of L, say $\{\ell_1, \ldots, \ell_n\}$. Then $\{\ell_i \alpha_i : 1 \leq i \leq n, 1 \leq j \leq d\}$ is a basis for V over K:

- Clearly it is a spanning set, as every element $\mu_j \in L$ can be written as $\sum_i^n \lambda_{ij}\ell_i$, so if $v \in V$ is represented as $\sum_j^d \mu_j \alpha_j$ it can also be represented as $\sum_j^d \sum_i^n \lambda_{ij}\ell_i\alpha_j$.
- It is also linearly independent - if $\sum_j^d \sum_i^n \lambda_{ij}\ell_i\alpha_j = 0$, then by independence of the α_j we must have $\sum_i^n \lambda_{ij}\ell_i = 0 \forall j$, and then by independence of the ℓ_i we have $\lambda_{ij} = 0 \forall i, j$

Hence, $\dim_K V = n \times d = \dim_L V \times [L : K]$ □

Corollary 1.6. *If L/K is a finite extension $\alpha \in L$, then α is algebraic over K and* $\deg_K \alpha | [L : K]$.

Proof. Immediate from the Tower Law: $L/K(\alpha)/K$ are field extensions. □

Examples:

1. If $[L : K] = p$, a prime, then $\forall \alpha \in L \setminus K, K(\alpha) = L$, as $[K(\alpha) : K] | p$, so is 1 or p. It is not 1 as $\alpha \notin K$, so $[L : K(\alpha)] = 1 \iff L = K(\alpha)$.
2. Every irreducible polynomial $f \in \mathbb{R}[x]$ has degree 1 or 2, as $\mathbb{C}$ is algebraically closed, so f has a root $\alpha \in \mathbb{C}$. $[\mathbb{C} : \mathbb{R}] = 2$, so $[\mathbb{R}(\alpha) : \mathbb{R}] = 1$ or 2, so $\deg f = 1$ or 2.
3. $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$. Then $[L : \mathbb{Q}] = 12$.

Proof. $L \supseteq \mathbb{Q}(\sqrt[3]{2})$. But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, since the minimal polynomial is $x^3 - 2$. Similarly $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 4$, so $3|[L : \mathbb{Q}]$ and $4|[L : \mathbb{Q}]$, hence $12|[L : \mathbb{Q}]$. Now $[L : \mathbb{Q}(\sqrt[3]{2})] \leq 4$, since the minimal polynomial $x^4 - 5$ is still a polynomial in $\mathbb{Q}(\sqrt[3]{2})$, and hence $[L : \mathbb{Q}] \leq 3 \cdot 4 = 12$, so $[L : \mathbb{Q}] = 12$]. □

4. Let $\omega = e^{2\pi \mathrm{i}/p}$ where p is an odd prime, and let $\alpha = \omega + \omega^{-1} = e^{2\pi \mathrm{i}/p} + e^{-2\pi \mathrm{i}/p}$. What is $\deg_{\mathbb{Q}} \alpha$? Observe that ω is a root of $f(x) = 1 + x + \ldots + x^{p-1}$, which is irreducible by application of Eisenstein to $f(x + 1)$. So $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$. Now clearly $\alpha = \omega + \omega^{-1} \in \mathbb{Q}(\omega)$, so we have field extensions $\mathbb{Q}(\omega)/\mathbb{Q}(\alpha)/\mathbb{Q}$, and hence $\deg_{\mathbb{Q}} \alpha | p - 1$. If we consider $[\mathbb{Q}(\omega) : \mathbb{Q}(\alpha)]$, we can note that $\alpha\omega = \omega^2 + 1$, so ω is a root of $x^2 - \alpha x + 1$, hence $[\mathbb{Q}(\omega) : \mathbb{Q}(\alpha)] = 1$ or 2. It is not 1 as $\omega \notin \mathbb{Q}(\alpha)$, and so $\deg_{\mathbb{Q}} \alpha = \frac{p-1}{2}$.

Corollary 1.7.

1. *$\alpha_1, \alpha_2, \ldots, \alpha_n$ are algebraic over K if and only if $[K(\alpha_1, \alpha_2, \ldots, \alpha_n) : K] < \infty$*
2. *If α, β algebraic over K then $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ (if $\beta \neq 0$) are algebraic over K.*

Proof.

1. $\Longleftarrow$: if $[K(\alpha_1, \ldots, \alpha_n) : K] < \infty$ then $\dim_K K(\alpha_i) < \infty$ so α_i algebraic over K.

   $\Longrightarrow$: α_n algebraic over K $\implies$ α_n algebraic over $K(\alpha_1, \ldots, \alpha_{n-1})$
   $\implies [K(\alpha_1, \ldots, \alpha_n) : K(\alpha_1, \ldots, \alpha_{n-1})] < \infty$.

   Hence by induction $[K(\alpha_1, \ldots, \alpha_n) : K] < \infty$, as it is product of finitely many finite integers.

2. This is immediate from *1* as $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha, \beta)$, which is a finite extension of K.

□

Corollary 1.8. *The elements of L which are algebraic over K form a subfield of L.*

Example: Let $a, b \in K$, and set $\alpha = \sqrt{a}, \beta = \sqrt{b}$. Let's try to define a polynomial satisfied by $\alpha + \beta = \gamma$. Compare powers of γ and use that $\alpha^2 = a, \beta^2 = b$ to simplify and look for linear relationships.

$$\begin{aligned} \gamma^2 &= \alpha^2 + 2\alpha\beta + \beta^2 = a + b + 2\alpha\beta \\ \gamma^4 &= (a+b)^2 + 4\alpha\beta(a+b) + 4\alpha^2\beta^2 \\ &= a^2 + 6ab + b^2 + 4\alpha\beta(a+b) \\ \therefore \gamma^4 - 2(a+b)\gamma^2 &= -(a-b)^2 \end{aligned}$$

So γ is a root of $x^4 - 2(a+b)x^2 + (a-b)^2$

Note that if $\deg_K \alpha = m, \deg_\alpha \beta = n$ then $K(\alpha, \beta)$ is spanned over K by monomials $\alpha^i \beta^j$ for $0 \leq i < m, 0 \leq j < n$. Hence for any $\gamma \in K(\alpha, \beta)$, the terms $1, \gamma, \ldots, \gamma^{mn}$ must be linear combinations over K over the monomials $\alpha^i \beta^j$, and, as there are $mn + 1$ of them they must be linearly dependent over K. However, they polynomial satisfied by X obtained in this way is in general not going to be the minimal polynomial.

Exercise: Show that, if m, n and mn are elements of $\mathbb{Q}$ and are not squares, then $[\mathbb{Q}(\sqrt{m} + \sqrt{n}) : \mathbb{Q}] = 4$.

An extension L/K is an ***algebraic extension*** if every $\alpha \in L$ is algebraic over K.

Example: $\overline{\mathbb{Q}} \coloneqq \{\alpha \in \mathbb{C} : \alpha \text{ algebraic over } \mathbb{Q}\}$ is an algebraic extension of $\mathbb{Q}$, but is not a finite extension of $\mathbb{Q}$, as $\sqrt[n]{2} \in \overline{\mathbb{Q}}$ so $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$ for all integers n.

Proposition 1.9.

1. *A finite extension is algebraic*
2. *$K(\alpha)/K$ is an algebraic extension $\implies$ α is algebraic over K*
3. *If $M/L/K$ are extensions then M/K is algebraic if and only if M/L and L/K are algebraic*

Proof.

1. Already done by **1.7**, as $1, \alpha, \alpha^2, \ldots$ cannot all be linearly independent, so α algebraic for all $\alpha \in L \supseteq K$.
2. $\alpha \in K(\alpha)$, so α is algebraic over K by definition.
3. $\Longleftarrow$: Suppose M/K is algebraic. Then if $\alpha \in M$, α is algebraic over K, so is algebraic over L, so M/L is algebraic, and moreover L/K is algebraic as $L \subseteq M$.

   $\Longrightarrow$: Let $\alpha \in M$. We know α is algebraic over L, so $r_0 + r_1\alpha + \ldots + r_d\alpha^d = 0$ for some $r_0, \ldots, r_d \in L$. Let $L_0 = K(r_0, \ldots, r_d)$. Each $r_l \in L$, and L is algebraic over K, so each r_l is algebraic over K. But this then implies $[L_0 : K] < \infty$. Now α is algebraic over L_0, so $[L_0(\alpha) : L_0] < \infty$. Hence the tower law now gives $[L_0(\alpha) : K] = [L_0(\alpha) : L_0][L_0 : K] < \infty$.

   But this then says that $\alpha \in L_0(\alpha)$, a finite extension of K, and hence α is algebraic over K as required.

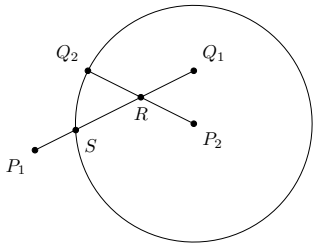
□

In other words, an extension L/K is algebraic if and only if it is a union of subfields, each of which is finite over K.

2 Euclidean Constructions - An Interlude

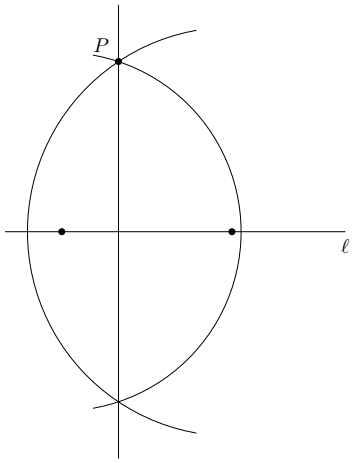
Using only Euclidean constructions, can we trisect angles in general? Can we construct a square with the same area as a given circle? Can we construct a cube with double the volume of an existing cube?

We start with two points, our "constructed points", called P, Q. Given P, Q, we can construct new points using the intersections of lines and circles through the constructed points. For instance, if P_1, P_2, Q_1, Q_2 are constructed points, we can then construct the points R, S in the diagram below:

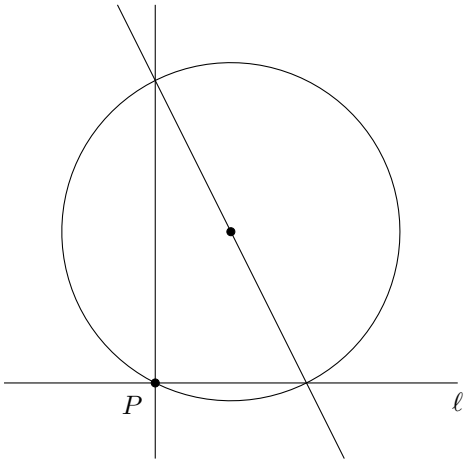


Things we can do here:

1. Draw a line through a constructed point P perpendicular to a line ℓ.

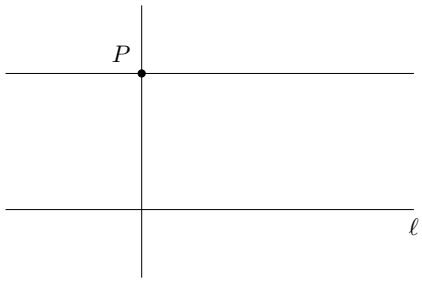


If $P \notin \ell$

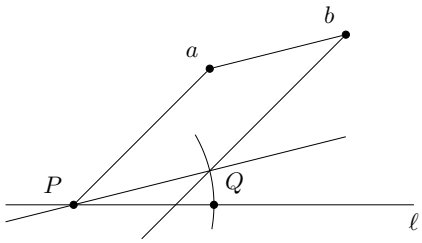


If $P \in \ell$

2. Draw a line parallel to ℓ, passing through a point P.



3. Mark off a length defined by two points on a constructible line starting at some point P.



$|PQ| = |ab|$

As a corollary of these, we can introduce Cartesian coordinates in the plane given our original two points, defining them to be the coordinates $(0,0)$ and $(0,1)$. We say that $\lambda \in \mathbb{R}$ is ***constructible*** if a line segment of length $|\lambda|$ is the distance between 2 constructible points.

Lemma 2.1. *$p = (a,b)$ is constructible if and only if $a, b \in \mathbb{R}$ are constructible.*

Proof. The forwards implication is trivial - simply drop perpendiculars onto both axes. Conversely, if a, b, are constructible, we can erect perpendicular on both axes distances of a, b from the origin, whose intersection is p. □

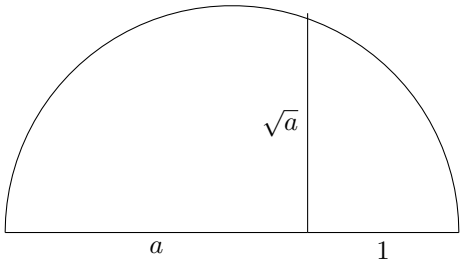
Proposition 2.2. *Constructible numbers form a subfield of $\mathbb{R}$.*

Proof. Suppose $a, b \in \mathbb{R}$ are constructible. Then $a + b$ is constructible by construction (3), as is $-a$.

We can also construct ab and a/b using similar triangles □

Proposition 2.3. *If $a > 0$ is constructible, so is $\sqrt{a}$.*

Proof.



□

Corollary 2.4. *Let $\mathbb{Q} \subseteq F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n = K \subseteq \mathbb{R}$ be a chain of subfields of $\mathbb{R}$ such that, for each $n \geq 0$, F_{n+1} is obtained from F_n but adjoining $\sqrt{r}$ for some $r \in F_n$ which is not a square in F_n. Then every element of K is constructible.*

Conversely, if $a_1, \ldots, a_n \in \mathbb{R}$ are constructible numbers, there is a chain of subfields as above with each $a_i \in K$.

Proof. By the preceding constructions, every element of K is constructible. For the converse, we start with $(0,0), (0,1) \in \mathbb{F}_0^2$. It is enough to show that the coordinates of the intersections of circles and lines either lie in the same field, or produce a field extension by adding $\sqrt{r}$ for some r. □

Corollary 2.5. *If $a \in \mathbb{R}$ is constructible, then a is algebraic, and $\deg_{\mathbb{Q}} a = 2^n$ for some $n \in \mathbb{N}_0$.*

The consequences of this are:

1. We cannot construct a cube with a volume of 2, as $\deg_{\mathbb{Q}} \sqrt[3]{2} = 3$, which is not a power of 2.

2. We cannot in general trisect an angle. Suppose we could trisect e.g. 60°, i.e. construct 20°. Firstly, we can construct 60°, as $\cos(60°) = 1/2 \in \mathbb{Q}$. Then we observe that $\cos(20°) = \alpha$ is not constructible. We can see that it is a root of $8x^3 - 6x - 1$, which is irreducible, and hence its degree is 3 which is not a power of 2.
3. A regular p-gon for p prime is not constructible by compass and straight edge if $p - 1$ is not a power of 2. This is because constructing one is the same as constructing $\cos(2\pi/p)$ which has degree $\frac{p-1}{2}$.
4. Squaring the circle is impossible, as it would involve constructing π, which is transcendental over $\mathbb{Q}$ (unless you are in Indiana in 1897).

3 Splitting Fields

Let $f \in K[x]$ be irreducible. Then $K[x]/(f)$ is a field, and we denote it by K_f. Then K_f/K is a field extension. We write $\alpha = x + (f)$ for the image of x in K_f. If $d = \deg(f)$, then $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ form a basis of K_f/K, and $f(\alpha) = f(x) + (f) = (f) = 0$ in K_f, so $K_f = K(\alpha)$, and α is a root of f in K_f. We say K_f is ***obtained from K by adjoining a root of f.***

Let $L/K, M/K$ be two field extensions of the same field K. A homomorphism of fields $\phi : L \hookrightarrow M$ which is the identity on K is called a ***K-homomorphism***. For instance, $\mathbb{C} \to \mathbb{C}; z \mapsto \overline{z}$ is an $\mathbb{R}$-homomorphism but not a $\mathbb{C}$-homomorphism.

Lemma 3.1. *Let L/K be an extension of fields, and $f \in K[x]$ be irreducible. There is a bijection:*

$$\{K - \textit{homomorphisms } \phi : K_f \to L\} \longleftrightarrow \textit{ roots of } f \textit{ in } L = \{\tilde{\alpha} \in L | f(\tilde{\alpha}) = 0\}$$

Proof. A K-homomorphism $K[x]/(f) \to L$ is the same thing as a ring homomorphism $\phi : K[x] \to L$ such that $\phi(r) = r$ for $r \in K$ and $\ker \phi = (f)$. But such a ϕ is determined by $\phi(x)$ as $\phi(\sum r_i x^i) = \sum r_i \phi(x)^i$.

Note that this shows $\phi(f(x)) = f(\phi(x))$, and so $\phi(f) = 0 \iff \ker \phi \supseteq (f) \iff \ker \phi = (f)$, as f is irreducible, so (f) is maximal.

Hence, if $\phi : K_f \to L$ is a K-homomorphism, put $\tilde{\alpha} = \phi(x) = \phi(x + (f))$. Then $\phi(f) = f(\tilde{\alpha}) = 0$, so $\tilde{\alpha}$ is a root of f in L, giving a map LHS $\to$ RHS.

Conversely, if $\tilde{\alpha}$ is a root of f in L, we've just showed there is a map $K[x] \to L$ sending $x \mapsto \tilde{\alpha}$, and it is clear that if $\tilde{\beta} \neq \tilde{\alpha}$ is another such root, the maps constructed are different. □

In particular, the number of K-homomorphisms $K_f \to L$ is finite, and equal to the number of distinct roots of f in L, which is $\leq \deg f$.

Corollary 3.2. *if $\alpha, \beta \in L$ are algebraic, then they have the same minimal polynomial over K if and only if there is a K-isomorphism $K(\alpha) \to K(\beta)$ sending α to β*

Proof. $K(\alpha) \xleftarrow{\sim} K_f = K[x]/f(x)$, where f is the minimal polynomial of α.

- $\implies$ If β has the same minimal polynomial, then $K(\beta) \xleftarrow{\sim} K_f$ also
- $\impliedby$ If there exists a K-isomorphism $\theta : K(\alpha) \xrightarrow{\sim} K(\beta)$ sending α to β, then this gives a K-homomorphism $K_f \to K(\beta)$, such that $f(\beta) = 0$, by the previous lemma. So if g is the minimal polynomial of β, then $g | f$. But α, β interchangeable, so $f | g$, and they are the same polynomial up to a unit.

□

Example: $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ irreducible. Let $\alpha = \sqrt[3]{2}$ be the real cube root of 2, and let $\omega = e^{2\pi \mathrm{i}/3} \in C$, so $\alpha, \alpha\omega, \alpha\omega^2$ are both roots of f. Then there is a $\mathbb{Q}$-isomorphism $\mathbb{Q}(\alpha) \xrightarrow{\sim} \mathbb{Q}(\alpha\omega)$, sending α to $\alpha\omega$. However, $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ whilst $\mathbb{Q}(\omega\alpha) \nsubseteq \mathbb{R}$. This is NOT a contradiction: the isomorphism sees the internal structure of the field, and not how they sit as subfields of $\mathbb{C}$.

Let $f \in K[x]$. A ***splitting field*** for f is a field extension L/K such that:

1. f splits into linear factors in $L[x]$
2. $L = K(\alpha_1, \ldots, \alpha_d)$ where $\alpha_1, \ldots, \alpha_d$ are the roots of f in L. Equivalently, f does not split into linear factors in any proper subfield of L containing K.

Examples: $K = \mathbb{Q}$

1. $f(x) = x^2 + 1 = (x + \mathrm{i})(x - \mathrm{i}) \implies \mathbb{Q}(\mathrm{i})$ is a splitting field for f.
2. $f(x) = x^3 - 2$. Claim: a splitting field is $\mathbb{Q}(\alpha, \alpha\omega) = \mathbb{Q}(\alpha, \omega)$.
   We can see this as $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]$ is divisible by $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3, [\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, and so divisible by 6, but the degree must be ≤ 6 as $\{1, \omega, \alpha, \alpha\omega, \alpha^2, \alpha^2\omega\}$ span $\mathbb{Q}(\alpha, \omega)$ as a $\mathbb{Q}$-vector space, and so $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6$, but adjoining any single root of f will by definition give an extension of degree 3.
3. The splitting field of any quadratic polynomial can be obtained by adjoining one root - exercise for the interested reader.
4. $f(x) = \frac{x^p - 1}{x - 1}, \omega = e^{2\pi \mathrm{i}/p}$. Then $\mathbb{Q}(\omega)$ is a splitting field for f over $\mathbb{Q}$.

Theorem 3.3. *Splitting fields exist, and are unique, but are not "uniquely unique".*

Proof of existence. Let $f \in K[x]$. Then a splitting field for f exists, by adjoining all roots of f. More precisely: we induct on $\deg f$, assuming that for any field a polynomial of degree $< \deg f$ has a splitting field. If $\deg f = 1$, we are done as f is a product of linear factors in $K[x]$. Otherwise, let g be an irreducible factor of f, and $K_g = K[t]/(g) = K(\alpha)$ where $\alpha = t + (g)$, so $f(\alpha = 0$ in K_g, i.e. $f(x) = (x - \alpha)f_1(x) \in K_g[x]$, and $\deg f_1 = \deg f - 1 < \deg f$. By the inductive hypothesis, a splitting field exists for f_1 over K_g, say $L = K_g(\alpha_2, \ldots, \alpha_n)$. Then we claim L is a splitting field for f over K, as f factors over L as $(f - \alpha)(f - \alpha_2) \ldots (f - \alpha_n)$. Moreover, $L = K(\alpha, \alpha_2, \ldots, \alpha_n)$. □

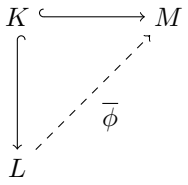
Example: $K = \mathbb{R}$ and we want to construct $\mathbb{C}$. Let $f(x) = x^2 + 1$.

1. The usual way is to let $\mathbb{C} = \mathbb{R}_f = \mathbb{R}[x]/(x^2 + 1)$ builds $\mathbb{C}$ with a distinguished element i, which is the image of x.
2. Let $g(y) = y^2 + 2y + 2 = (y + 1 - \mathrm{i})(y + 1 + \mathrm{i})$. Then we could let $\mathbb{C} = \mathbb{R}_g = \mathbb{R}[y]/(y^2 + 2y + 2)$, with a distinguished element, the image of y. However, there is no canonical way to choose what y is: it could be $-1 + \mathrm{i}$ or $-1 - \mathrm{i}$.

Hence we have two $\mathbb{R}$-homomorphisms $\mathbb{R}[y]/(y^2 + 2y + 2) \xrightarrow{\sim} \mathbb{R}[x]/(x^2 + 1)$, as we can map $y \mapsto -x - 1$ or $y \mapsto x - 1$, and we have no reason to prefer one over the other. In general, we will show that whilst the splitting fields might be unique, the K-homomorphisms to these splitting fields are not unique.

Proof of uniqueness. Let $f \in K[x]$, and L be the splitting field for f. Suppose $\phi : K \hookrightarrow M$ is the inclusion map of fields where $M \supseteq L$, and $\phi(f)$ splits in M.

Then we can extend ϕ to a homomorphism $\overline{\phi} : L \to M$, factoring $K \hookrightarrow M$:



Moreover,

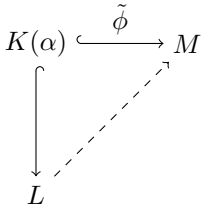
1. The number of such extensions is $\leq [L : K]$, and equals $[L : K]$ if f does not have multiple roots (note f has multiple roots in M if and only if f has multiple roots in L).
2. If M is a splitting field, any such $\overline{\phi}$ is an isomorphism, which we prove by induction on $[L : K]$:

   If f splits into linear factors over K, i.e. $[L : K] = 1$, we are done. Otherwise, let $\alpha_1 \in L \backslash K$ be a root of

   $$, and$$

   be the minimal polynomial of α_1 over K, so that $g|f$. Then by lemma **3.1**, there is a bijection between the K-homomorphisms with $K(\alpha_1) \to M$ and the roots of $\phi(g)$ in M. So, since $\phi(f)$ splits in M, $\phi(g)$ also splits, and tehre are $\leq [K(\alpha_1 : K]$ such homomorphisms, with equality if there are no repeated roots of g.

   Now, by the induction hypothesis,

   where $[L : K(\alpha)] < [L : K]$, there exists an extension $\overline{\phi}$ of $\tilde{\phi}$, and the number of such extensions is $\leq [L : K(\alpha)]$. Hence, the total number of such extensions is $\leq [L : K(\alpha)][K(\alpha : K] = [L : K]$ by the tower law, with equality if there is no repeated roots.
3. If M is a splitting field, $M = K(\beta_1, \ldots, \beta_d)$ where β_l are roots of f. But, if $\overline{\phi} : L \to M$ are extensions as above, and $\alpha_1, \ldots, \alpha_d$ are roots of f in L, then $\overline{\phi}(\alpha_1), \ldots, \overline{\phi}(\alpha_d)$ are the roots of f in M, so are exactly $\beta_1, \ldots, \beta_d$ and hence $\overline{\phi}$ is surjective. It is injective, as homomorphisms of fields are injective.

□

4 Finite Fields

Proposition 4.1. *Let K be a field and $G \subseteq K^*$ be a finite subgroup. Then G is cyclic.*

Proof. G is abelian, so the structure theorem for finite abelian groups gives that:

$$G = \mathbb{Z}/(m_1) \times \ldots \times \mathbb{Z}/(m_r) \text{ where } m_1|m_2, m_2|m_3, \ldots, m_{r-1}|m_r$$

and $|G| = m_1 \cdot m_2 \cdot \ldots \cdot m_r$.

So if $\alpha \in G$, $\alpha^{m_r} = 1$, this is every element of G is a root of the the polynomial $x^{m_r} - 1$. But, the number of roots of $x^{m_r} - 1$ is $\leq m_r$. The only that this holds, i.e. that $m_1 \cdot \ldots \cdot m_r \leq m_r$ is if $m_1 = m_2 = \ldots = m_{r-1} = 1$, and so K is a finite a field, so $|K| = q = p^r$ for some prime p, and K^* is a cyclic group isomorphic to $\mathbb{Z}/(p^r - 1)$ □

For instance, $\mathbb{F}_7^\times = \langle 3 \rangle = \{3, 2, 6, 4, 5, 1\}$. Note that there is no canonical isomorphism , and so no canonical generator.
For an alternate proof of this, see Number Theory.

Lemma 4.2 (Fermat's Little Theorem)**.** *Let K be a finite field, and $|K| = q$. Then every $\alpha \in K$ satisfies $\alpha^q = \alpha$, that is α is a root of $x^q - x$, and $x^q - x$ factors into linear factors with distinct roots*

Proof. This is clear if $x = 0$. If $\alpha \neq 0, \alpha \in K^*$, a cyclic group of order $q-1$, so $\alpha^{q-1} = 1$. Finally, a polynomial of degree d has at most d roots, but we have found q distinct roots of $x^q - x$. □

So this shows that K is the splitting field of $x^q - x \in \mathbb{F}_p[x]$, given that we know K exists. Conversely, given $q = p^r$, we want to construct a finite field with q elements. We will define it as the splitting field of $x^q - x \in \mathbb{F}_p[x]$. However, we need to know that $x^q - x$ has distinct roots - this will require a proof.

If K is a field, we can define $\frac{d}{dx} : K[x] \to K[x]$ to be the linear map $x^n \mapsto nx^{n-1}$, the ***formal derivative***.

Proposition 4.3.

- *Leibnitz rule:* $\frac{d}{dx}(fg) = \frac{df}{dx}g + f\frac{dg}{dx}$
- *Chain rule:* $\frac{d}{dx}(f \circ g) = \frac{df}{dx}(g(x))\frac{dg}{dx}$

Proof. An exercise for the reader. □

We write $f'(x)$ for $\frac{df}{dx}$ if there is no confusion.

Lemma 4.4. *If L/K is a field extension, $f \in K[x]$, $\alpha \in L$ a root of f so that $f(\alpha) = 0$. Then α is a simple root if and only if $f'(\alpha) \neq 0$.*

Proof. $f(x) = (x-\alpha)g(x) \implies f'(x) = (x-\alpha)g'(x) + g(x)$, and hence $g(\alpha) = 0 \iff f'(\alpha) = 0$.
In particular, f has multiple roots if and only if $\deg \gcd(f, f') > 0$. □

Proposition 4.5. *Let R be a ring and* $\operatorname{char} R = p$*. Then the map $F : x \mapsto x^p$ is a ring homomorphism, call the* **Frobenius map**.

Proof. We must show that $F(x + y) = F(x) + F(y)$. But $(x + y)^p = x^p + \binom{p}{1}x^{p-1}y + \ldots + \binom{p}{p-1}xy^{p-1} + y^p$, and $p|\binom{p}{i}$ for $1 \leq i \leq p - 1$, so we are one. □

Theorem 4.6 (Finite fields exist and are unique)**.** *Let $q = p^n$ for p prime and $n \geq$. Then:*

- *There exists a field F_q with $\#F_q = q$. Moreover, any two such fields are isomorphic.*
- *F_q is the splitting field of $x^q - x \in F_p[x]$.*
- *F_q contains a subfield of order p^k if and only if $k|n$.*

Proof.

2. $\Longrightarrow$ 1. This is immediate.

2. Let K be the splitting field of $x^q - x$, so that $K = \mathbb{F}_p(\alpha_1, \ldots, \alpha_q)$ where $\alpha_i^q = \alpha_i$. We must show that $\#K = q$.

We claim: If α, β are roots of $x^q - x$, then so is $\alpha + \beta, \alpha\beta, \alpha/\beta$ (if $\beta \neq 0$).

Proof. F is a ring homomorphism, so $(\alpha + \beta)^{p^n} = (\alpha^p + \beta^p)^{p^{n-1}} = \ldots = \alpha^{p^n} + \beta^{p^n}$. □

This implies that the field generated by the roots of $x^q - x$ is just the union of these roots, so $\#K \leq q$. But if α is a root $f(x) = x^q - x$, then α is not a root of $f'(x) = qx^{q-1} - 1 = -1$ as $q = p^r = 0$. Hence $x^q - x$ has q distinct roots, so $\#K \geq q$, and hence $\#K = q$.

$\Longrightarrow$ 3. If $K \subseteq \mathbb{F}_q$ and $\#K = p^k$, then $[K : \mathbb{F}_p] = k$, and the tower law gives $k|n$.

$\Longleftarrow$ 3. It is enough to show that $x^{p^k} - x | x^{p^n} - x$ if $k|n$ as then $\left\{\alpha \in \mathbb{F}_q | \alpha^{p^k} = \alpha\right\}$ is the desired subfield, by *2.*

But $x^r - q | x^{rs} - 1$, as $y^s - 1 = (y-1)(1 + y + \ldots + y^{s-1})$, it is enough to show that $p^k - 1 | p^{k\ell} - 1$ if $n = k\ell$. But this follows from the previous line.

□

Examples:

$\mathbb{F}_4$: $x^4 - x = x(x-1)(x^2 + x + 1)$. Now $(x^2 + x + 1)$ is irreducible over $\mathbb{F}_2$, and so $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$. Notice that $\mathbb{F}_2 \subseteq \mathbb{F}_4$ as we see $x^2 - x | x^4 - x$.

$\mathbb{F}_8$: $x^8 - x = x(x-1)(x^6 + x^5 + \ldots + 1)$, where this polynomial is irreducible over $\mathbb{Z}[x]$, but in $\mathbb{F}_2[x]$ is $x(x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$. These two cubic factors are all of the irreducible polynomials of degree 3 over $\mathbb{F}_2$. So we see that the 6 elements of $\mathbb{F}_8 \setminus \mathbb{F}_2$ fall into two classes: those which are roots of these two cubics.

Note that $[\mathbb{F}_8 : \mathbb{F}_2] = 3; [\mathbb{F}_4 : \mathbb{F}_2] = 2$, so $\mathbb{F}_4 \nsubseteq \mathbb{F}_8$.

Also, $\mathbb{F}_8[x] = \mathbb{F}_2[x]/(x^3 + x + 1)$, and we have that $1, \beta, \beta^2$ form a basis of $\mathbb{F}_8$ over $\mathbb{F}_2$, where $\beta^3 = \beta + 1$.

Observe that if $f \in \mathbb{F}_p[x]$ is irreducible and $\deg f = n$, then $K =: \mathbb{F}_p[x]/(f)$ is a field, $[K : \mathbb{F}_p] = n$ so $\#K = p^n =: q$. But then $x^q - x$ splits completely in K, and its roots are all the elements of K, and hence $f(x) | x^q - x$. That is, every irreducible polynomial in $\mathbb{F}_p[x]$ of degree n divides $x^{p^n} - x$.

Proposition 4.7. *Let f be irreducible. Then $f | x^q - x$ if and only if* $\deg f | n$.

Proof. An exercise for the reader. □

From this point of view, if you try to define $\mathbb{F}_q$ as $\mathbb{F}_p[x]/(f)$, f an irreducible polynomial of degree n, the difficulty is in showing that such a polynomial actually exists.