Galois Theory

November 19, 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.

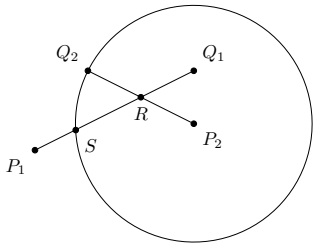
□

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

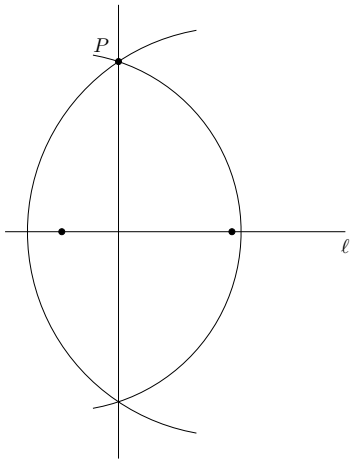
Using only Euclidean constructions, can we trisect angles in general? Can we construct a square with the same area as a given circle? Can we construct a cube with double the volume of an existing cube?

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:

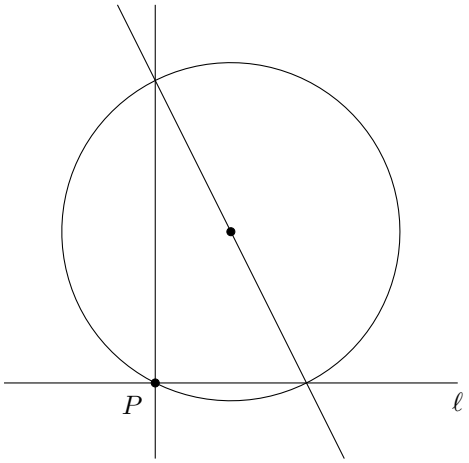


Things we can do here:

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

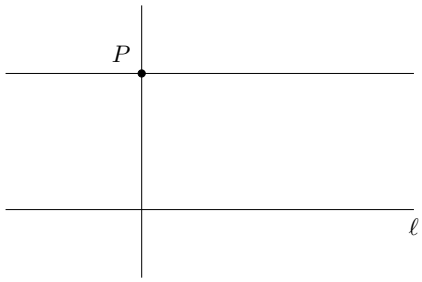


If $P \notin \ell$

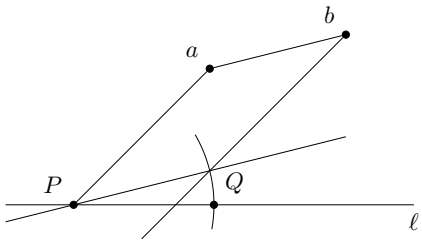


If $P \in \ell$

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. □

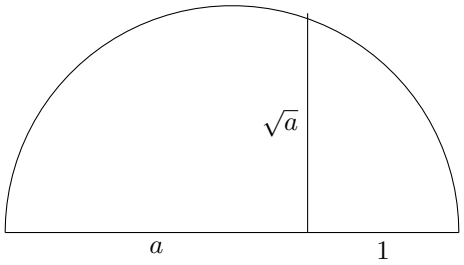
Proposition 2.2. *Constructible numbers form a subfield of $\mathbb{R}$.*

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

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

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 $\widetilde{\alpha} = \phi(x) = \phi(x + (f))$. Then $\phi(f) = f(\widetilde{\alpha}) = 0$, so $\widetilde{\alpha}$ is a root of f in L, giving a map LHS $\to$ RHS.

Conversely, if $\widetilde{\alpha}$ is a root of f in L, we've just showed there is a map $K[x] \to L$ sending $x \mapsto \widetilde{\alpha}$, and it is clear that if $\widetilde{\beta} \neq \widetilde{\alpha}$ 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. $K(\alpha) \widetilde{\leftarrow} K_f = K[x]/f(x)$, where f is the minimal polynomial of α.

- $\implies$ If β has the same minimal polynomial, then $K(\beta) \widetilde{\leftarrow} K_f$ also
- $\impliedby$ If there exists a K-isomorphism $\theta : K(\alpha) \widetilde{\to} K(\beta)$ 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 $\omega = e^{2\pi \mathfrak{i}/3} \in C$, so $\alpha, \alpha\omega, \alpha\omega^2$ are both roots of f. Then there is a $\mathbb{Q}$-isomorphism $\mathbb{Q}(\alpha) \widetilde{\longrightarrow} \mathbb{Q}(\alpha\omega)$, 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. $f(x) = x^2 + 1 = (x + \mathfrak{i})(x - \mathfrak{i}) \implies \mathbb{Q}(\mathfrak{i})$ 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. $f(x) = \frac{x^p - 1}{x - 1}, \omega = e^{2\pi \mathfrak{i}/p}$. 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 $f(x) = x^2 + 1$.

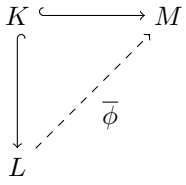
1. The usual way is to let $\mathbb{C} = \mathbb{R}_f = \mathbb{R}[x]/(x^2 + 1)$ builds $\mathbb{C}$ with a distinguished element $\mathfrak{i}$, which is the image of x.
2. Let $g(y) = y^2 + 2y + 2 = (y + 1 - \mathfrak{i})(y + 1 + \mathfrak{i})$. Then we could let $\mathbb{C} = \mathbb{R}_g = \mathbb{R}[y]/(y^2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

Hence we have two $\mathbb{R}$-homomorphisms $\mathbb{R}[y]/(y^2 + 2y + 2) \widetilde{\longrightarrow} \mathbb{R}[x]/(x^2 + 1)$, 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,

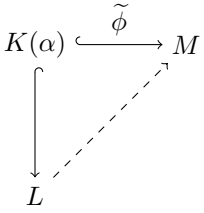
1. The number of such extensions is $\leq [L : K]$, and equals $[L : K]$ if f does not have multiple roots (note f has multiple roots in M if and only if f has multiple roots in L).
2. If M is a splitting field, any such $\overline{\phi}$ is an isomorphism, which we prove by induction on $[L : K]$:

   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 $\widetilde{\phi}$, 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.

Separable Extensions

Let K be a field, and $\operatorname{char} K = p, b \in K$ an element which is not a p^{th} power in K. For instance let $K = \mathbb{F}_p(y)$ for y transcendental, then take $b = y$. Consider the polynomial $f(x) = x^p - b \in K[x]$, and let L be the splitting field for F over K, and $\alpha \in L$ be a root of f, so that $\alpha^p = b$. Observe that $f'(x) = px^{p-1} = 0$ as $p = 0$ in K, so α must be a multiple root. In fact $x^p - b = x^p - \alpha^p = (x-\alpha)^p$, so α is a root p times. Moreover, f is irreducible as, if not, then $(x-\alpha)^m$ is an irreducible factor of f for some $0 < m < p$.

But then $(x-\alpha)^m = x^m - m\alpha x^m + \ldots + (-\alpha)^m \in K[x]$, but then $m\alpha \in K$, but $K \ni m \neq 0 \implies \alpha \in K$, and so b is a p^{th} power $\lightning$.

Hence $\mathbb{F}_p(y^{1/p})/\mathbb{F}_p(y)$ is a very strange extension as the minimal polynomial for $\alpha = y^{1/p}$ has multiple roots.

We say that $f \in K[x]$ is ***separable*** if it splits into <u>distinct</u> linear factors in a splitting field. Otherwise it is ***inseparable***. For instance, $x^9 - x \in \mathbb{F}_p[x]$ is separable, but $x^p - y \in F_p(y)[x]$ is inseparable.

In other words, f is separable if and only if $\gcd(f, f') = 1$.

Proposition 4.8.

1. *Let $f \in K[x]$ be an irreducible polynomial. Then f is separable if and only if $f' \neq 0$.*
2. *If* $\operatorname{char} K = 0$*, then every irreducible polynomial over K is separable.*
3. *If* $\operatorname{char} K = p$*, then if $f \in K[x]$ is irreducible, then (f is inseparable $\iff$ $f(x) = g(x^p)$ for some $g \in K[x]$).*

Proof.

1. Without loss of generality, we can assume f is monic. Then as f is irreducible the gcd of f, f' is 1 or f, since $\gcd | f$.

   If $f' = 0$, then $\gcd(f, 0) = f$ and so f is inseparable.
   If $f' \neq 0$, then $\deg f' < \deg f$, and hence $\deg \gcd(f, f') < \deg f$, so is 1, and so f is separable.

2. Let $f(x) = \sum r_i x^i$ irreducible. Then $f'(x) = \sum i r_i x^{i-1}$, and so $f'(x) = 0 \implies ir_i = 0$ for all $i \geq 1$. But $\operatorname{char} K = 0 \implies r_i = 0$, and hence f is constant, and not an irreducible polynomial.

3. As above, $ir_i = 0$ for all $i \geq 1$. $\operatorname{char} K = p$ implies that $r_i = 0$ for all i with $p \nmid i$, and hence $f(x) = \sum r_{pi} x^{pi} = g(x^p)$ where $g(x) = \sum r_{pi} x^i$.

□

Let α be algebraic over K. We say α is ***separable*** if the minimal polynomial of α over K is separable, and otherwise ***inseparable***.

We say that L/K is a ***separable extension*** if all $\alpha \in L$ are algebraic and separable over K.

For instance, if $\operatorname{char} K = 0$ then all algebraic extensions are separable. However, $\mathbb{F}_p(y^{1/p})/\mathbb{F}_p(y)$ is not separable.

Then we have:

Lemma 4.9. *Let α be algebraic over K with minimal polynomial $f \in K[x]$, and let L/K be an extension in which f splits. Then:*

$$\alpha \text{ is separable over } K \iff \text{there are exactly } \deg f \text{ } K\text{-homomorphisms } K(\alpha) \to L$$

Proof. This is immediate from the Key Lemma **3.1**. □

Proposition 4.10. *Suppose α is algebraic and separable over K. Then $K(\alpha)/K$ is separable.*

Proof. Let $\beta \in K(\alpha)$, and f be the minimal polynomial of α over K, g be the minimal polynomial of β over K, and let $\deg g = m$.

Let M be a splitting field for fg, in particular, M is an extension in which g splits. We need to show that there are precisely $m = \deg g$ K-homomorphisms $K(\beta) \to M$.

We have that $K \subseteq K(\beta) \subseteq K(\alpha)$, and let $n = [K(\alpha) : K(\beta)]$ so that $[K(\alpha) : K] = nm$.

Consider the map $\{\phi : K(\alpha) \to M; \phi \text{ a } K\text{-homo}\} \to M\{\overline{\phi} : K(\beta) \to M; \phi \text{ a } K\text{-homo}\}$, where $\overline{\phi} \coloneqq \phi|_{K(\beta)}$.

As α is separable over K, the size of the LHS is $[K(\alpha) : K] = mn$, and also the size of the RHS is at most $[K(\beta) : K] = m$, with equality if and only if β is separable over K. α separable over K implies α is separable over $K(\beta)$, so there are exactly n $K(\beta)$-homomorphisms from $K(\alpha) \to M$ extending $\overline{\phi}$. But that says that exactly n K-homomorphisms map to each $\overline{\phi}$ and so the size of the RHS is $\geq mn/n = m$, and hence must be m, and we are done by **4.9**. □

Corollary 4.11. *$\mathbb{F}_q/\mathbb{F}_p$ is a separable extension.*

Proof. This follows immediately by above, and was also clear by last lecture's proof. □

Proposition 4.12. *Let M/L be a finite separable extension, and likewise L/K. Then M/K is a finite separable extension.*

Proof. We will deduce this from an interesting theorem, the "Theorem of the primitive element", which implies that, if L/K is a finite separable extension, then $L = K(\alpha)$ for some $\alpha \in L$. So $M = L(\beta)$ for some $\beta \in M$, so $M = K(|alpha, \beta)$ which we will see implies $M = K(\gamma)$ for some γ. Then it is enough to show that γ is separable over K. Then by the tower law, $[K(\gamma) : K] = [K(\gamma) : K(\alpha)] \cdot [K(\alpha) : K] =: n \cdot m$, and we can let T be a field in which all the roots of the minimal polynomials of α, β, γ split.

α is separable over K implies that there are m distinct K-homomorphisms $K(\alpha) \to T$, and β separable over $K(\alpha)$ gives n distinct K-homomorphisms from $K(\gamma) \to T$ extending each of the

$K(\alpha)$-homomorphisms from $K(\alpha) \to T$, and hence there are mn distinct K-homomorphisms from $K(\gamma) \to T$, and so γ is separable. $\square$

Lemma 4.13. *Let L/K be a field extension, and f, g polynomials over K. Then $\gcd(f,g)$ is the same whether you compute it in $K[x]$ or $L[x]$.*

Hence, the $\operatorname{lcm}(f,g) = f \cdot g / \gcd(f,g)$ is also independent of where you compute it.

Moreover, the lcm of a finite set of separable polynomials is also separable.

Proof. For the first part, let $h = \gcd_K(f,g), h' = \gcd_L(f,g)$. Then $h|f, h|g$ in $K[x]$ and so $h|f$ and $h|g$ in $L[x]$, and so $h|h'$ in $L[x]$ by definition. But $h = pf + qg$ for some $p, q \in K[x]$, and so $h'|h$ in $L[x]$ also. Hence $h = h'$.

For the second part, by above we can compute the lcm in any extension, so we choose an extension in which all the polynomials split into linear factors, so they split into distinct linear factors. But then the lcm is simply the product of all the distinct linear factors among these, which must be separable by construction. $\square$

Theorem 4.14 (The Theorem of the Primitive Element)**.** *Let $L = K(\alpha_1, \ldots, \alpha_n, \beta)$ be a finite extension of K, and suppose each of $\alpha_1, \ldots, \alpha_n$ is separable over K. Then there exists a $\gamma \in L$ such that $L = K(\gamma)$.*

Proof. If $|K| < \infty$, then $|L| < \infty$ also, and so L^* is a cyclic group. IF we choose γ to be a generator of L^*, then $L = K(\gamma)$.

If $|K|$ is infinite, then we induct on n. It is enough to show that $K(\alpha, \beta) = L$ with α separable over K and β arbitrary, as then $K(\alpha, \beta) = K(\beta_1)$ for some β_1, and so $K(\alpha_1, \alpha_2, \beta) = K(\beta_2)$ for some β_2, and so on.

Taking $L = K(\alpha, \beta)$, α separable, $|K| < \infty$, we will show that for *most* $c \in K$ the subfield $K(\gamma)$ with $\gamma = \beta + c\alpha$ is all of L It is enough to show that $\alpha \in K(\gamma)$, as then $\beta = \gamma - c\alpha \in K(\gamma)$ so $L \supseteq K(\gamma) \supseteq K(\alpha, \beta) = L$. We will do this by determining the minimal polynomial of α over $K(\gamma)$.

Let f be the minimal polynomial of α and g the minimal polynomial of β, and M a splitting field for fg, so that $f(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$ for the α_i all distinct, $\alpha = \alpha_i$ for some i, and $g(x) = (x - \beta_1)(x - \beta_2)\ldots(x - \beta_m)$.

Consider $h(x) = g(\gamma - cx) \in K(\gamma)[x]$. By definition, $h(\alpha) = g(\beta) = 0$. But $f(\alpha) = 0$ also, so $(x - \alpha) | \gcd(f,h)$. If we can show $\gcd(f,h) = x - \alpha$, then $x - \alpha = A \cdot f + B \cdot h \in K(\gamma)[x] \implies -\alpha \in K(\gamma)$

In order to compute $\gcd_{K(\gamma)}(f,h)$, by the lemma it suffices to compute $\gcd_M(f,h)$. It suffices to show that $h(\alpha_i) \neq 0$ for $i = 2, \ldots, n$. But $h(\theta) = \iff g(\gamma - c\theta) = 0 \iff \gamma - c\theta = \beta_j$ for some j, as $\beta_1, \ldots, \beta_m$ are roots of g.

But $\gamma = \beta + c\alpha$, so $h(\alpha_i) = 0 \iff \exists\ j$ s.t. $\beta_j - \beta = c(\alpha - \alpha_i)$. So if $c \notin \left\{ \frac{\beta_j - \beta}{\alpha - \alpha_i} | i > 1, j \right\}$, a finite set, then $h(\alpha_i) \neq 0 \forall i$, and $K(\gamma) = L$. But we assumed that $|K| = \infty$, so there is such a c, and hence such a γ. $\square$

Corollary 4.15. *If L/K finite and separable then $L = K(\gamma)$ for some $\gamma \in L$, and in particular if L/K is finite and $\operatorname{char} K = 0$ then $L = K(\gamma)$ for some $\gamma \in L$.*

For example, if $K = \mathbb{Q}[\mathrm{i}, \sqrt[3]{2}]$, so $[K : \mathbb{Q}] = 6$.
In the notation of the proof, $\beta_i = \mathrm{i}, \beta_2 = -\mathrm{i}, \alpha_1 = \sqrt[3]{2}, \alpha_2 = \omega\sqrt[3]{2}, \alpha_3 = \omega^2\sqrt[3]{2}, \omega = e^{\mathrm{i}2\pi/3}$

Then $K = \mathbb{Q}[\mathrm{i} + c\sqrt[3]{2}]$ if $c \neq 0, c \in \mathbb{Q}$, and $c \neq \frac{\pm\mathrm{i}-\mathrm{i}}{\sqrt[3]{2}(\omega^{\pm 1}-1)}$. Note that all of these elements are not in $\mathbb{Q}$, and so $K = \mathbb{Q}[\mathrm{i} + c\sqrt[3]{2}]$ for $c \in \mathbb{Q} \setminus \{0\}$.

As noted, many, and indeed most, elements of K will generate K, for example $\mathrm{i}\sqrt[3]{2}$ is a generator.

As another example, let $K = \mathbb{F}_p(x, y), L = \mathbb{F}_p(x^{1/p}, y^{1/p}) = K[z, w]/(z^p - x, w^p - y)$. We claim that if $\gamma \in L$ then $K(\gamma) \neq L$. Note that this does not satisfy the preconditions of the theorem of the primitive element. It is enough to show that $\gamma^p \in K$ as then $[K(\gamma) : K] \leq p$ but $[L : K] = p^2$. But $\gamma = \sum a_{ij}x^{i/p}y^{j/p}$ with $a_{ij} \in K$, so $gamma^p = \sum a_{ij}^p x^i y^j \in K$.

5 Algebraic Closure

K is ***algebraically closed*** if every non-constant polynomial $f \in K[x]$ has a root in K, and hence splits in K.

Lemma 5.1. *The following are equivalent:*

1. *K is algebraically closed.*
2. *Let L/K be an extension and $\alpha \in L$ algebraic over K. Then $\alpha \in K$.*
3. *L/K an algebraic extension implies $L = K$.*

Proof. This is obvious (apparently). □

Some examples of algebraically closed fields are $\mathbb{C}$ and $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} : \alpha \text{ algebraic over } \mathbb{Q}\}$.

Example: What is an algebraic closure of $\mathbb{F}_p$? Choose a sequence r_i of positive integers such that $r_i | r_{i+1}$ and every $n \in \mathbb{N}$ divides r_i for some i, for instance $r_i = i!$. We have seen that $\mathbb{F}_{p^{r_i}} \subseteq \mathbb{F}_{p^{r_{i+1}}}$, so we can choose embeddings $\mathbb{F}_{p^{r_1}} \hookrightarrow \mathbb{F}_{p^{r_2}} \hookrightarrow \ldots \hookrightarrow \mathbb{F}_{p^{r_n}} \hookrightarrow \ldots$. Then define $\bar{\mathbb{F}}_p := \cup\mathbb{F}_{p^{r_i}}$. We claim that $\bar{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$.

Proof. It is clear that $\bar{\mathbb{F}}_p$ is algebraic over $\mathbb{F}_p$. So we must show that if $f \in \bar{\mathbb{F}}_p[x]$ then f factors into linear factors in $\bar{\mathbb{F}}_p[x]$. We can write $f = \sum^N a_i x^i$ with $a_0, \ldots, a_N \in \mathbb{F}_q$ for $q = p^{r_i}$ for some i.

But a splitting field exists for f and it is a finite extension of $\mathbb{F}_q$, so it is isomorphic to a field $\mathbb{F}_{p^N}$ for some N. By construction, $\mathbb{F}_{p^N} \hookrightarrow \mathbb{F}_p^{r_i}$ for some i, and so f splits into linear factors in $\mathbb{F}_{p^{r_i}}[x] \subseteq \bar{\mathbb{F}}_p[x]$. □

The following theorem can be proven using similar ideas and Zorn's lemma:

Theorem 5.2. *Every field K has an algebraic closure L, and if L_1, L_2 are algebraic closures of K then there is a K-isomorphism $\phi : L_1 \to L_2$. However, ϕ is not unique.*

6 Galois Extensions

So far we've looked at properties of $K(\alpha)/K$ which depend on a single root α of its minimal polynomial f, and maps $K(\alpha) \to K[x]/(f)$.

What about the other roots of f, and how do they interact?

Let L/K be a field extension. Then $\mathrm{Aut}(L/K) = \{phi : L \to L : \phi \text{ a } K\text{-homo and isomorphism}\}$, or equivalently the set of field isomorphisms $\phi : L \to L$ such that $\phi(k) = k$ for every $k \in K$.

$\mathrm{Aut}(L/K)$ measures the failure of isomorphisms to be unique. If $\phi : M \to L$ is a K-isomorphism, and $\sigma \in \mathrm{Aut}(L/K)$, then $\sigma \circ \phi$ is another K-isomorphism. Conversely, if $\phi_1, \phi_2 : M \to L$ are K-isomorphisms, then $\phi_1\phi_2^{-1} \in \mathrm{Aut}\, L/K$ and is non-trivial if and only if $\phi_1 \neq \phi_2$. Note that $\mathrm{Aut}(L/K)$ is a group.

Examples:

1. L/K is an extension and $[L : K] = 2$, $\mathrm{char}\, K \neq 2, L = K(\alpha)$. Then the minimal polynomial $f(x) = x^2 + bx + c = (x - \alpha)(x - \alpha')$ in the splitting field of f. Then $\alpha + \alpha' = b, \alpha\alpha' = c$, and so since $\alpha \in L, \alpha' = b - \alpha$ is in L as well, so L is a splitting field, and so $L = K(\alpha')$ as well.

   Now the key lemma says that there exists a K-homomorphism $\sigma : L \to L; \alpha \mapsto \alpha'$, which is a field isomorphism. Note that $\sigma \neq \mathrm{id} \iff \alpha \neq \alpha'$. But if $\alpha = \alpha'$ then $2\alpha = b \implies \alpha = b/2 \in K$ as $\mathrm{char}\, K = 2$, and so $[L : K] = 1 \neq 2$.

   Hence $\mathrm{Aut}(L/K) = \mathbb{Z}_2$.
   Note that this is the case for $\mathrm{Aut}(\mathbb{Q}[i]/\mathbb{Q}), \mathrm{Aut}(\mathbb{C}/\mathbb{R}), \mathrm{Aut}(\mathbb{Q}(1 + \sqrt{2})/\mathbb{Q})$.
   Warning: $\mathbb{Q}(1 + \sqrt{2}) \subseteq \mathbb{R}$, but σ is not a continuous automorphism with respect to the topology induced from $\mathbb{R}$. We we are seeing is this as a field extension and not with any structure induced from being a subfield of $\mathbb{R}$.

2. $L = \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. The minimal polynomial $f(x) = x^3 - 2$, which splits in $\mathbb{C}[x]$ as $(x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)$ where $\alpha = \sqrt[3]{2}, \omega = e^{2\pi \mathrm{i}/3}$. Observe that $\omega\alpha, \omega^2\alpha \notin L$. So the key lemma tells us that $\mathrm{Aut}(L/K) = 1$, as there are no K-homomorphisms $\mathbb{Q}(\alpha) \to L$ other than $\alpha \mapsto \alpha$.

3. $L = K(x)/K$. We claim that $\mathrm{Aut}(L/K) = PGL_2(K)$, the group of Möbius transformations. Proof is an exercise.

4. L/K is quadratic, $L = K(\alpha)/K$. If the minimal polynomial of f has distinct roots, then $\mathrm{Aut}(L/K) = \mathbb{Z}_2$, and this always happens if $\mathrm{char}\, K \neq 2$. If $\mathrm{char}\, K = 2$, then we have distinct roots when $\alpha^2 \notin K$, otherwise $\mathrm{Aut}(L/K) = 1$.

L/K is ***biquadratic*** if $[L : K] = 4$ and $\mathrm{char}\, K \neq 2$. Then L is generated by two elements of degree 2, so $L = K(\alpha, \beta)$ with $\alpha^2 = a, \beta^2 = b$. It's clear that there is a unique $K(\alpha)$-isomorphism $L \to L$ sending $\beta \mapsto -\beta$, which we call σ_β. Similarly we have σ_α. It's clear that $\sigma_\alpha\sigma_\beta = \sigma_\beta\sigma_\alpha, \sigma_\alpha^2 = 1, \sigma_\beta^2 = 1$, and so $\mathbb{Z}_2 \times \mathbb{Z}_2 \leq \mathrm{Aut}(L/K)$. The key lemma tells us that there are no other K-automorphisms, and any K-automorphism $L \to L$ must permute both the roots of $x^2 - a$ and $x^2 - b$, and so $\mathrm{Aut}(L/K) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Lemma 6.1. *Let L/K be a field extension and $f \in K[x], \sigma : L \to L$ be a K-homomorphism of L.*

1. *Then if $\alpha \in L$ has $f(\alpha) = 0$ then $f(\sigma(\alpha)) = 0$ also.*

2. *Suppose* $L = K(\alpha_1, \ldots, \alpha_n)$ *and* σ *is a* K*-homomorphism* $L \to L$ *with* $\sigma\alpha_i = \alpha_i$ *for all* i*. Then* $\sigma = \mathrm{id}$*.*

3. *Let* L *be a splitting field for* f *with roots* $\alpha_1, \ldots, \alpha_n$*. Then* $\mathrm{Aut}(L/K) \leq S_n =$ *permutations of* $\alpha_1, \ldots, \alpha_n$*.*

Proof. 1 and 2 are clear, and 3 follows from these 2. □

Lemma 6.2. *Moreover,* L/K *is separable.*

Proof. Let $\alpha \in L$. We must show that the minimal polynomial of α over K has distinct roots in a splitting field. Let $G\alpha = \{\sigma\alpha : \sigma \in G\} = \{\alpha_1, \ldots, \alpha_r\}$ be the orbit of α, so that α_i are distinct, and let $g(x) = \Pi_{i=1}^r (x - \alpha_i)$. By definition, g has distinct roots, and $g(\alpha) = 0$, and if $\sigma \in G$ then σ permutes $\{\alpha_1, \ldots, \alpha_r\} = G\alpha$, and so $\sigma g(x) = g(x)$, and hence $g(x) \in K[x]$. Hence, if $f \in K[x]$ is the minimal polynomial of α then $f | g$, and as g has distinct roots, so does f. □

Lemma 6.3. *Let* $\gamma \in L$*. Then the minimal polynomial of* γ *is* $g(x) = \Pi_{\alpha \in G\gamma}(x - \alpha)$*. In particular* $\deg_K \gamma = \#G\gamma$*.*

Proof. We have already shown that $g(x) = K[x], g(\gamma) = 0$ and the minimal polynomial divides g. It remains to show that $g(x)$ is irreducible. But if not, $g = g_1 \cdot g_2$, and in $L[x]$ we have $g_1(x) = \Pi_{\alpha \in A}(x - \alpha), g_2(x) = \Pi_{\alpha \in B}(x - \alpha)$, and $A \cup B = G\gamma, A \cap B = \emptyset$. But $g_i \in K[x]$ and so each of A, B are G-stable, which is not possible if both are nonempty. □

Example: Let $L = \mathbb{Q}(\mathfrak{i}, \sqrt{2}), G = \mathbb{Z}/2 \times \mathbb{Z}/2 = \mathrm{Aut}(L/\mathbb{Q}), K = \mathbb{Q}$. This is as we have $\sigma_1 : \mathfrak{i} \mapsto -\mathfrak{i}; \sigma_2 : \sqrt{2} \mapsto -\sqrt{2}$. Then if $\gamma = \mathfrak{i}$, we have $G\mathfrak{i} = \{\pm\mathfrak{i}\} \implies$ minimal polynomial for $\mathfrak{i}$ is $(x + \mathfrak{i})(x - \mathfrak{i}) = x^2 + 1$ irreducible. If $\gamma = \mathfrak{i} + \sqrt{2} + 1$, then the minimal polynomial for γ is $(x - 1 - \mathfrak{i} - \sqrt{2})(x - 1 + \mathfrak{i} - \sqrt{2})(x - 1 - \mathfrak{i} + \sqrt{2})(x - 1 + \mathfrak{i} + \sqrt{2}) \in \mathbb{Q}[x]$. This is computationally very easy to find, as long as we know the automorphism group.

Lemma 6.4. $[L : K] < \infty, K = L^G$

Proof. Choose $\alpha \in L$ such that $[K(\alpha) : K]$ is maximal. This is possible by lemma one, which says that $[K(\alpha) : K] \leq \#G$. Now let $\beta \in L$. We show that $\beta \in K(\alpha)$, i.e. $K(\alpha) = L$. But $[K(\alpha, \beta) : K(\alpha)] \leq [K(\beta) : K] \leq \#G < \infty$. Hence $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\beta)][K(\beta) : K] < \infty$.

Moreover, $K \subseteq K(\alpha, \beta) \subseteq L$, so $K(\alpha, \beta)/K$ is separable, since L/K is separable. We then apply the theorem of the primitive element to see that $K(\alpha, \beta) = K(\gamma)$ for some γ, and hence $[K(\gamma) : K] = [K(\alpha) : K]$ by maximality of $[K(\alpha) : K]$, and so $[K(\gamma) : K(\alpha)] = 1$, i.e. $\beta \in K(\alpha)$ as required. □

Theorem 6.5 (Artin)**.** *Let* L *be a field,* $G \leq \mathrm{Aut}(L)$ *be a finite group. Then:*

1. $[L : L^G] = \#G$
2. $G = \mathrm{Aut}(L/L^G)$

Proof.

1. By the previous lemma, $L = K(\gamma)$ for some γ, and $\deg_K \gamma = \#G\gamma$. We claim that $\#G\gamma = \#G$. Equivalently, $\mathrm{stab}_G(\gamma) = \{1\}$. To see this, observe that $K(\gamma)$ is a vector space over K with basis $1, \gamma, \gamma^2, \ldots$. Hence if $\sigma \in G$ acts trivially on γ, then $\sigma\gamma = \gamma$, and so σ acts trivially on all of L, i.e. $\sigma\ell = \ell \forall \ell \in L$. But $G \leq \mathrm{Aut}(L)$ acts faithfully on L by definition, and so such a σ is the identity.

   Alternatively, simply observe that $[L : K] \leq \#G$ by the previous lemma, but $\#G \leq [L : K]$ by linear independence of field automorphisms, so we have the result by trichotomy.

2. $G \leq \mathrm{Aut}(L/K)$, and so $K = L^G \supseteq L^{\mathrm{Aut}(L/K)} \supseteq K$. Hence $L^{\mathrm{Aut}(L/K)} = K$, and so $G = \mathrm{Aut}(L/K)$.

□

Note that this theorem is very useful for computing examples:
Example: $L = \mathbb{C}(y), G = \langle \sigma, \tau \rangle, \sigma y = \mathrm{i}/y, \tau y = -y$. Then what is $K = L^G$. Firstly, G is $\mathbb{Z}_2 \times \mathbb{Z}_2$ as $\sigma^2 y = y, \tau^2 y = y, \sigma\tau y = -\tau\sigma y$, and $Gy = \{y, -y, \mathrm{i}/y, -\mathrm{i}/y\}$, and hence the minimal polynomial of y over K is $(x-y)(x+y)(x-\mathrm{i}/y)(x+\mathrm{i}/y) = (x^2-y^2)(x^2+y^{-2}) = x^4+x^2(y^{-2}-y^2)+1 \in K[x]$. So we must have that $y^2 - y^{-2} \in K$. We know that $\deg_K(y) = 4$ and even that $\deg_{\mathbb{C}(\omega)}(y) = 4$, so we heave that $K = \mathbb{C}(\omega)$ where $\omega = y^2 + y^{-2}$.

Example: $L = \mathbb{F}_{q^n}, K = \mathbb{F}_q$. Then we claim $\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \mathbb{Z}_n$.

Proof. Let $\phi(x) = x^9$ for all $x \in \mathbb{F}_{q^n}$. Then if $x \in \mathbb{F}_q$, as $x^9 = x$ we have $\phi(x) = x$, and so $\phi \in \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ defines a map $\mathbb{Z} \to \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q), i \mapsto \phi^i$. But then $\phi^n(x) = x^{q^n} = x$ for all $x \in \mathbb{F}_{q^n}$, and there is some $x \in \mathbb{F}_{q^n}$ with $\phi^i(x) \neq x$ if $x < n$ as $(\mathbb{F}_{q^n})^{\phi^i} = \mathbb{F}_{q^i}$, and hence $\mathbb{Z}_n = \langle \phi \rangle \hookrightarrow \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. But then $\#\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q) = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ by Artin's theorem, and hence we have equality. □

Proposition 6.6. *Let L/K be a finite extension. Then $\#\mathrm{Aut}(L/K) | [L : K]$, with equality if and only if L/K is Galois.*

Proof. Set $M = L^{\mathrm{Aut}(L/K)}$, so that we have a tower $K \leq M \leq L$. Artin's theorem gives us that $[L : M] = \#\mathrm{Aut}(L/K)$, and so by the tower law $[L : K] = \#\mathrm{Aut}(L/K)[M : K]$. □

Theorem 6.7. *L/K is Galois if and only if L is the splitting the field of a separably polynomial over K. More precisely, the following are equivalent:*

1. *L/K is Galois*
2. *$G \leq \mathrm{Aut}(L)$ is a finite subgroup and $K = L^G$*
3. *L is the splitting field of a separable polynomial in $K[x]$*
4. *L/K is separable and the minimal polynomial over K of each $\alpha \in L$ splits into linear factors in $L[x]$*

Proof.

1. $\Longrightarrow$ 2. Trivial

2. $\Longrightarrow$ 1. Follows immediately from Artin

2. $\Longrightarrow$ 4. The linear factors have roots $\{\sigma\alpha | \sigma \in G\}$

4. $\Longrightarrow$ 3. If $L = K(\alpha_1, \ldots, \alpha_n)$, let f_i be the minimal polynomial of each α_i which is separable over L, and so the lowest common multiple of $f_1, \ldots, f_n$ is a separable polynomial with L as its splitting fields.

3. $\Longrightarrow$ 1. If L is the splitting field of a polynomial $f \in K[x]$. Then the key lemma tells us that the number of K-homomorphisms $L \to L$ is less than or equal to $[L : K]$, and as f is separable we have equality. But this then says that $\#\operatorname{Aut}(L/K) = [L : K]$, and so our previous proposition says L/K is Galois.

□

Corollary 6.8. *Any finite separable extension L/K is centered in a Galois extension $K \subseteq L \subseteq N$ with N/K Galois.*

Proof. Let $L = K(\alpha_1, \ldots, \alpha_n)$ and set N to be the splitting field of the lowest common multiple of all the minimal polynomials of the α_i. This is separable by definition, and N/K is Galois by the previous theorem, and no proper subfield containing K is Galois.

Moreover, if $K \subseteq L \subseteq N'$ with N'/K Galois but no proper subfield containing K is Galois, then there exists an L-automorphism $N \to N'$. □

Corollary 6.9. *If $K \subseteq M \subseteq L$ and L/K is Galois, then L/M is Galois.*

Proof. Property *4.* from **6.7** holds for L/K and so it holds for L/M. □

Theorem 6.10 (Fundamental Theorem of Galois Theory)**.** *If L/K is a Galois extension and $G = \operatorname{Aut}(L/K)$, then there is bijection:*

$$\begin{aligned} &\textit{((subgroups of } G\textit{))} \to \textit{((fields } M \textit{ with } K \subseteq M \subseteq L\textit{))} \\ &H \mapsto L^H \end{aligned}$$

with inverse given by $\operatorname{Aut}(L/M) \hookleftarrow M$. In particular, there are only finitely many intermediate fields.

Examples:

1. If $G = \mathbb{Z}_p$ then the tower law implies there are no non-trivial subfields, and there are also clearly no non-trivial subgroups.
2. If $L = \mathbb{F}_{q^n}, K = \mathbb{F}_q$, then $G = \operatorname{Aut}(L/K) = \mathbb{Z}_n$. L/K is Galois from last lecture, and so we know that the only subfields of L are $\mathbb{F}_{q^m}$ for $m|n$.
3. $L = \mathbb{Q}(\mathfrak{i}, \sqrt{2}) \supseteq K = \mathbb{Q}$. We've already seen that the only subgroups of $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ are $\langle\sigma, \tau\rangle, \langle\sigma\rangle, \langle\tau\rangle, \mathbb{1}$, and so the theorem tells us that the only proper subfields are $\mathbb{Q}(\mathfrak{i}\sqrt{2}), \mathbb{Q}(\mathfrak{i}), \mathbb{Q}(\sqrt{2})$.

Proof. We check the composition of these two maps in both directions is the identity:

- $H \mapsto L^H \mapsto \operatorname{Aut}(L/L^H) = H$ by Artin's theorem
- $M \mapsto \operatorname{Aut}(L/M) \mapsto L^{\operatorname{Aut}(L/M)}$. But the corollary showed L/M is Galois, so Artin gives $L^{\operatorname{Aut}(L/M)} = M$.

□

Theorem 6.11 (Properties of the Galois correspondence)**.**

1. *It is order reversing: if* $H \subseteq H'$*, then* $L^{H'} \subseteq L^H$*. If* $M \subseteq M'$*, then* $\mathrm{Aut}(L/M') \leq \mathrm{Aut}(L/M)$
2. *A subgroup* $H \leq G$ *is normal if and only if* $K \subseteq L^H$ *is a Galois extension. That is,* $K \subseteq M$ *is Galois if an only if* $\mathrm{Aut}(L/M) \trianglelefteq \mathrm{Aut}(L/K)$*, and in that case* $\mathrm{Aut}(M/K) = G/H$*. Note that this is a group if and only if* H *is normal.*

Proof. Suppose $N \trianglelefteq G$ is normal. If $n \in N, \sigma \in G, \ell \in L^N$, then $n\sigma(\ell) = \sigma\sigma^{-1}n\sigma(\ell) = \sigma n'\ell = \sigma\ell$, and so $\sigma(\ell) = \ell$, i.e. $\sigma(L^N) \subseteq L^N$, and so we have a map $G/N \to \mathrm{Aut}(L^N/K)$. But the set of all σ such that $\sigma/L^N = 1$ is the automorphism group $\mathrm{Aut}(L/L^n) = N$ by Artin's theorem, and so we have an injection $G/N \hookrightarrow \mathrm{Aut}(L^N/K)$, and so $\#\mathrm{Aut}(L^N/K) \geq \#G/N$.

But $K \subseteq L^N \subseteq L$, and $\#\mathrm{Aut}(L^N/K) \leq \#G/N$, and hence we have equality, so $[L^N : K]$ is Galois. □

Example: $x^3 - 3x + 1$. $D = -4 \cdot (-3)^3 - 27 \cdot 1^2 = 81 = 3^4$, and so the Galois group $\mathrm{Gal}(f) = A_3$, as 3^4 is a square in $\mathbb{Q}$.

Note that if $f(x)$ is a cubic over $\mathbb{Q}$ with only one real root then its splitting field's Galois group is S_3, since then we can adjoin a real root and then two complex roots.

Compare the cubic and quadratic equation. $f(x) = x^2 + bx + c \in K[x]$, which factors somewhere as $(x - \alpha_1)(x - \alpha_2)$ with $\alpha_1 + \alpha_2 = b, \alpha_1\alpha_2 = c$. Now setting $D = (\alpha_1 - \alpha_2)^2 = b^2 - 4c$. But $b^2 - 4c$ is not a square if an only if $\alpha_1, \alpha_2 \notin K \iff \mathrm{Gal}(f) = S_2$, otherwise the roots of f are in K and $\mathrm{Gal}(f) = \mathbb{1} = A_2$.

Proposition 6.12. *$f(x) \in K[x]$ irreducible with L/K a splitting field with* $\mathrm{char}\, K \neq 2$*. Let $f(x) = (x - \alpha_1)\dots(x - \alpha_n)$ in $L[x]$. Set $D = \Pi_{i<j}(\alpha_i - \alpha_j)^2$. Then $D \in K$ and:*

1. *$D \neq 0 \iff f$ separable*
2. *D is a square in $K \iff \mathrm{Gal}(f) \subseteq A_n$*
3. *D is a polynomial in the coefficients of f*

Proof. 1. is clear. As for *2.*, let $\delta = \Pi_{i<j}(\alpha_i - \alpha_j), \delta^2 = D, G = \mathrm{Gal}(f) \subseteq S_n, \delta \neq 0 \iff f$ separable. If $\sigma \in G, \sigma\delta = \begin{cases} \delta & \sigma \in A_n \\ -\delta & \sigma \notin A_n \end{cases}$. So $G \subseteq A_n \iff \forall \sigma \in G, \sigma\delta = \delta \iff \delta \in L^G = K \iff D = \delta^2 \in K$ is a square in K.

Part *3.* requires proof, and is why this is useful, but we will prove a more general version of this later on. □

7 Symmetric Polynomials

Let R be a ring, and $R[z_1, \dots, z_n]$ be a polynomial ring in n indeterminates. S_n acts on $R[z_1, \dots, z_n]$ by permuting the z_i, i.e. for $w \in S_n, z_i \mapsto z_{wi}$ where $(123)z_1 = z_2$ e.g.

Then $R[z_1, \dots, z_n]^{S_n} = \{f \in R[z_1, \dots, z_n] : wf = f \forall w \in S_n\}$, the symmetric polynomials.

For instance, $e_1 = z_1 + z_2 + \ldots + z_n$ is a symmetric polynomial. Or we could have $e_2 = \sum_{i<j} z_i z_j$, or $e_3 = \sum_{i<j<k} z_i z_j z_k$, all the way up to $e_n = z_1 \ldots z_n$. These are called the elementary symmetric functions.

Theorem 7.1 (Fundamental Theorem of Symmetric Polynomials)**.** *Every symmetric polynomial can be written uniquely as a polynomial in $e_1, \ldots, e_n$. More precisely, the map of rings $R[w_1, \ldots, w_n] \to R[z_1, \ldots, z_n]^{S_n}; w_i \mapsto e_i$ is an isomorphism.*

For instance, $sumz_i^2 = e_1^2 - 2e_2$.

We use this: K is a field, $f \in K[x]$, L a splitting field for f and $f(x) = (x - \alpha_1) \ldots (x - \alpha_n)$. If $f(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \ldots \pm a_n$, then $a_1 = e_1(\alpha_1, \ldots, \alpha_n), a_2 = e_2(\alpha_1, \ldots, \alpha_n)$ all the way up to $a_n = e_n(\alpha_1, \ldots, \alpha_n)$, and so any polynomial in $\{a_1, \ldots, a_n\}$ is a symmetric function of $\alpha_1, \ldots, \alpha_n$, and the theorem says that the converse is also true, that any symmetric function of $\alpha_1, \ldots, \alpha_n$ can be written as a polynomial in the coefficients of f.

For example, if $\Delta(f) = \Pi_{i<j}(\alpha_i - \alpha_j)^2$ is the discriminant of f, then the theorem says there is some polynomial in $e_1, \ldots, e_n$, $\Delta(e_1, \ldots, e_n)$ equal to $\Pi_{i<j}(z_i - z_j)^2$, sending $e_1 \mapsto -a_1$.

We claim $\Delta(x^2 + px + q) = -4p^3 - 27q^2$, and so $\Delta(f) = \Pi_{1 \le i < j \le 3}(z_i - z_j)^2$ is a homogeneous polynomial of degree 6. But note that $e_1 \mapsto 0$, and so it must be a linear combination of e_2^3 and e_3^2. On the other hand, Δ vanishes if f has repeated roots, so consider $f(x) = (x - \alpha)^2(x + 2\alpha)$. Then $-27c + 4d = 0$. Finally calculate $\Delta(x^3 - x) = 4$ by explicit computation, so $d = -27, c = -4$.

Proof. We need some notation. Given $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{N}^n$, we write $z^\lambda = z_1^{\lambda_1} \ldots z_n^{\lambda_n}$. It is clear that $\{z^\lambda : \lambda \in \mathbb{N}^n\}$ is a basis of $R[z_1, \ldots, z_n]$.

We can then totally order $\mathbb{N}^n$ by lexicographic order. Observe that if λ is in decreasing order, i.e. $\lambda_1 \ge \lambda_2 \ge \ldots \ge \lambda_n$, then $\lambda \ge \omega\lambda$ for all $\omega \in S_n$.

Hence every orbit $S_n\widetilde{\lambda}$ has a maximal element λ which is $\widetilde{\lambda}$ reordered so that $\lambda_1 \ge \lambda_2 \ge \ldots \ge \lambda_n$.

From this we can deduce that $\{\sum_{\mu \in S_n \lambda} z^\mu : \lambda = (\lambda_1 \ge \ldots \ge \lambda_n) \in \mathbb{N}^n\}$ is a basis of $R[z_1, \ldots, z_n]^{S_n}$, as linear independence comes from the fact that different λs have disjoint monomials in $\omega\lambda$, and the span comes from the argument above.

Let $f \in R[z_1, \ldots, z_n]^{S_n}$. Write $f = cz^\lambda + \ldots$, where the other terms are z^μ for $\mu < \lambda$.

Then $f = cz_1^{\lambda_1 - \lambda_2}(z_1 z_2)^{\lambda_2 - \lambda_3} \ldots (z_1 z_2 \ldots z_n)^{\lambda_n} + \ldots$

We claim now that $e_1^{\lambda_1 - \lambda_2} e_2^{\lambda_2 - \lambda_3} \ldots e_{n-1}^{\lambda_{n-1} - \lambda_n} e_n^{\lambda_n} = z_1^{\lambda_1 - \lambda_n} \ldots (z_1 \ldots z_n)^{\lambda_n} + \ldots$, which can be seen by carefully expanding it out.

Hence $f - ce_1^{\lambda_1 - \lambda_2} \ldots e_n^{\lambda_n}$ is a polynomial in terms z^μ with $\mu < \lambda$, as in $R[z_1, \ldots, z_n]^{S_n}$, so by induction we are done for surjectivity. □

Example: $\sum_{i \ne j} z_i^2 z_j^2 = z_1^2 z_2 + \ldots = z_1(z_1 z_2) + \ldots$..

Now $e_1 e_2 = \sum_{i,j<k} z_i z_j z_k = \sum_{i=j<k} + \sum_{j<k=i} = \sum_{\ne j,k}$.

Hence $e_1 e_2 = \sum_{i \ne j} z_i^2 z_j + 3e_3$.

Proof ctd (injectivity). Suppose $g \in R[w_1, \ldots, w_n]$ is such that $g(e_1, \ldots, e_n) = 0$ in $R[z_1, \ldots, z_n]^{S_n}$. We want to show that $g = 0$ by induction on n. Note that if $n = 1$ there is nothing to show as $R[z_1]^{S_1} = R[z_1]$

Otherwise, $g(e_1, \ldots, e_n) \in R[z_1, \ldots, z_n]$ is a polynomial in $z, \ldots, z_n$, and we can set $z_n = 0$. When we do this, $e_i|_{z_n=0} = e_i^0$ is e_i for one less variable if $i < n$ and 0 if $i = n$.

This says that $g(e_1^0, \ldots, e_{n-1}^0, 0)$ is 0 in $R[z_1, \ldots, z_{n-1}]^{S_{n-1}}$, and so by the inductive hypothesis, $g(w_1, \ldots, w_{n-1}, 0)$ is 0 in $R[w_1, \ldots, w_{n-}]$.

But this says that $g(w_1, \ldots, w_n) = w_n h(w_1, \ldots, w_n)$ for some polynomial $h \in R[w_1, \ldots, w_n]$, so $e_n h(e_1, \ldots, e_n)$ is 0 in $R[z_1, \ldots, z_n]^{S_n}$. But then $e_n = z_1 \ldots z_n \neq 0$ and $R[z_1, \ldots, z_n]$ is an integral domain so has no zero divisors, hence $h(e_1, \ldots, e_n) = 0$ in $R[z_1, \ldots, z_n]^{S_n}$. Now assume that g was of minimal degree mapping to 0 - this gives h of smaller degree mapping to 0, a contradiction. □

Lemma 7.2. *Let $L = K(z_1, \ldots, z_n)$ be the fraction field of $K[z_1, \ldots, z_n]$. Then we have:*

$$L^{S_n} \coloneqq (\operatorname{Frac} K[z_1, \ldots, z_n])^{S_n} = \operatorname{Frac}(K[z_1, \ldots, z_n]^{S_n})$$

Proof. $\supseteq$ is clear. For $\subseteq$ let $\gamma \in L^{S_n}, \gamma = f/g$ for f, g in $K[z_1, \ldots, z_n]$. Let $\mu = \Pi_{\sigma \in S_n} \sigma g \in K[z_1, \ldots, z_n]^{S_n}$. Then $\gamma\mu = f\Pi_{\sigma \in S_n, \sigma \neq 1} \sigma g \in K[z_1, \ldots, z_n]$ and is an S_n-invariant.

Hence $\gamma = \gamma \frac{\mu}{\mu} \in \operatorname{Frac}(K[z_1, \ldots, z_n]^{S_n})$ as required. □

Note that Artin implies that $[L : L^{S_n}] = n!$, and L/L^{S_n} is Galois.

Corollary 7.3. *Any finite group G is the Galois group of some field extension.*

Proof. By Cayley embed G inside S_n for some n (e.g. G acts on itself by left multiplication). Then the Galois correspondence gives that $G = \operatorname{Aut}(L/L^G)$ where $L = K(z_1, \ldots, z_n)$. □

If $d|n$ then $x^d - 1 | x^n - 1$ in $K[x]$ and even in $\mathbb{Z}[x]$, and if we divide $x^n - 1$ by all these obvious factors, we get $\Phi_n(x)$ then n^{th} cyclotomic polynomial. More precisely, every $\alpha \in \mu_n$, the n^{th} roots of unity, is a primitive d^{th} root of unity for precisely one $d|n$, namely $d = \operatorname{ord}(\alpha)$, and every primitive d^{th} root is an n^{th} root of 1 for $d|n$, so we have:

$$x^n - 1 = \Phi_n(x) \prod_{d|n, d \neq n} \Phi_d(x)$$

or equivalently,

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} \Phi_d(x)}$$

giving an inductive definition of $\Phi_n(x)$.

For example:

$$x^8 - 1 = (x^4 + 1)(x^4 - 1) = \underbrace{(x-1)}_{\Phi_1}\underbrace{(x+1)}_{\Phi_2}\underbrace{(x^2+1)}_{\Phi_4}\underbrace{(x^4+1)}_{\Phi_8}$$

$$x^6 - 1 = (x^3 + 1)(x^3 - 1) = \underbrace{(x-1)}_{\Phi_1}\underbrace{(x^2+x+1)}_{\phi_3}\underbrace{(x+1)}_{\Phi_2}\underbrace{(x^2-x+1)}_{\Phi_6}$$

This also shows us that $\Phi_n(x) \in \mathbb{Z}[x]$.

Theorem 7.4. *$\Phi_n(x) \in \mathbb{Q}[x]$ is irreducible.*

Dedekind, 1857. Recall Gauss's lemma: if $f \in \mathbb{Z}[x]$ which is monic factors properly in $\mathbb{Q}[x]$, then it also factors properly in $\mathbb{Z}[x]$. As $\Phi_n(x) \in \mathbb{Z}[x]$ is monic, we may suppose the theorem is false, i.e. $\Phi_n = f \cdot g$, where $f, g \in \mathbb{Z}[x]$.

We want then to show that, if ξ is a root of f, we have ξ^a is a root of f for all $a < n, (a, n) = 1$, and then all roots of Φ_n are roots of f and hence Φ_n is irreducible.

But a is a product of primes, say $p_1, \ldots, p_r$, with $p_i \nmid n$, so it is enough to show that ξ a root of f implies that ξ^p is a root of f if $p \nmid n$ where p is prime.

Suppose otherwise: as ξ^p is a primitive n^{th} root of 1, $\Phi_n(\xi^p) = f(\xi^p)g(\xi^p) = 0$. Since we are in a domain, $g(\xi^p) = 0$, and so ξ is a root of both $f(x)$ and $g(x^p)$, so they have a common factor of say $h(x)$ where $\deg h \geq 1$. Now we reduce mod p.

If $f(x) = \sum a_i x^x \in \mathbb{Z}[x]$, define $\bar{f}(x) = \sum \bar{a_i} x^i \in \mathbb{Z}_p[x]$, where $\bar{a_i} = a_i \mod p$.

One can check that $f \mapsto \bar{f}$ is a homomorphism of rings.

Now $\bar{g}(x^p) = (\bar{g}(x))^p$ as this is the Frobenius morphism.

Hence $h|f \implies \bar{h}|\bar{f}$, and $h|g(x^p) \implies \bar{h}|\bar{g}^p$. So some irreducible factor $\gamma|h$ divides $\bar{g}$, so $\gamma|(\bar{f}, \bar{g})$.

But then $\bar{\Phi_n}$ has a multiple root, but $p \nmid n$, so $\bar{\Phi_n}$ is a separable polynomial $\lightning$. □

Corollary 7.5. *If $K = \mathbb{Q}, L = \mathbb{Q}(\xi)$, then $[L : \mathbb{Q}] = \#(\mathbb{Z}/n\mathbb{Z})^*$, and $\chi : \mathrm{Aut}(L/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ is an isomorphism.*

If we write $\mathbb{Q}(\xi_n)$ for the n^{th} cyclotomic field, the extension of $\mathbb{Q}$ by a primitive n^{th} root of 1 called ξ_n, then this is the splitting field of $x^n - 1$.

We've shown that $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = (\mathbb{Z}/n\mathbb{Z})^*$, so the fundamental theorem of Galois theory says that for all subgroups $H \leq (\mathbb{Z}/n\mathbb{Z})^*$, we have an intermediate field $M = \mathbb{Q}(\xi_n)^H$, and as $(\mathbb{Z}/n\mathbb{Z})^*$ is abelian, in fact $H \trianglelefteq G$, so we have $M/\mathbb{Q}$ is Galois with Galois group $(\mathbb{Z}/n\mathbb{Z})^*/H$.

So now the natural thing to consider is the structure of $(\mathbb{Z}/n\mathbb{Z})^*$, and the corresponding subfields.

Examples:

1. $n = p$, a prime. Then $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{F}_p^* \cong \mathbb{Z}_{p-1}$. Then there is a unique intermediate subfield $\mathbb{Q} \subseteq M \subseteq \mathbb{Q}(\xi_n)$ with $[M : \mathbb{Q}] = k$ for each $k|(p-1)$.
   (a) $p = 5$, so we have $\mathbb{Z}_4$, giving a unique intermediate field of degree 2 over $\mathbb{Q}$. It is generated by $\xi + \xi^{-1} = \frac{1}{2}(-1 + \sqrt{5})$, and so we have $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{5}) \subsetneq \mathbb{Q}(\xi_5)$.

      More generally,

      Lemma 7.6. *For any $n \geq 3$, the unique subfield $M \leq \mathbb{Q}(\xi_n)$ with $[M : \mathbb{Q}] = \frac{\#(\mathbb{Z}/n\mathbb{Z})^*}{2}$ is $M = \mathbb{Q}(\cos(2\pi/n)) = \mathbb{Q}(\eta)$, where $\eta = \xi + \xi^{-1}$. In particular, $2|\#(\mathbb{Z}/n\mathbb{Z})^*$.*

      Proof. By the fundamental theorem of Galois theory, there is some unique M with $[\mathbb{Q}(\xi) : M] = 2$. But ξ is a root of the quadratic polynomial $x^2 - \eta x + 1 = 0$, and so

$[\mathbb{Q}(\xi) : \mathbb{Q}(\eta)] \leq 2$. But note that complex conjugation fixes $\mathbb{Q}(\eta)$ but not $\mathbb{Q}(\xi)$, hence $\mathbb{Q}(\xi) \neq \mathbb{Q}(\eta)$, so $M = \mathbb{Q}(\eta)$. □

(b) $p = 7$. $\#(\mathbb{Z}/7)^* = 6$, so choose a generator σ of $(\mathbb{Z}/7)^*$, for instance $\sigma = 3$. We already know that $\eta = \xi_7 + \xi_7^{-1}$ has degree $3 = 6/2$ over $\mathbb{Q}$. So what is its irreducible polynomial?

$\langle \sigma^3 \rangle = \mathbb{Z}/2$, so $\sigma^3 \eta = \eta$, so the orbit of η under $\langle \sigma \rangle$ is $\xi + \xi^{-1} = \eta, \xi^2 + \xi^{-2} = \eta_2, \xi^3 + \xi^{-3} = \eta_3$.

So $(x - \eta)(x - \eta_2)(x - \eta_3)$ is a polynomial in $\mathbb{Q}[x]$ irreducible, which expands out to $x^3 + x^2 - 2x - 1$. We also know there is a subfield $M' \subseteq \mathbb{Q}(\xi_7)$ with $[\mathbb{Q}(\xi_7) : M'] = 3$. We can field it by examining the orbit of σ^2 on ξ_7, since $\langle \sigma^2 \rangle = \mathbb{Z}/3$. If we put $\epsilon = \xi + \xi^2 + \xi^4$, then $\epsilon \in \mathbb{Q}(\xi_7)^{\mathbb{Z}_3} = M'$, so $\mathbb{Q}(\epsilon)$ is a quadratic extension of $\mathbb{Q}$, and $G.\epsilon = \{\epsilon, \epsilon'\}$ where $\epsilon' = \xi^{-1} + \xi^{-2} + \xi^{-4}$.

So the polynomial of this extension is $(x-\epsilon)(x-\epsilon') = x^2+x+2 \implies \mathbb{Q}(\epsilon) = \mathbb{Q}(\sqrt{-7})$, since the discriminant of this polynomial is $\Delta = 1 - 4 \cdot 2 = -7$.