M3/4/5 P11 - Galois Theory

April 29, 2015

Contents

Preface

v14.4.2
This document is based on the Galois Theory Course taught by Professor Kevin Buzzard at Imperial College London in Autumn 2014.
Thanks to Samuel Colvin, Gregory McElhinney and Nicholas Rome for the notes.
Thanks to Eamonn Postlethwaite for proof-reading Chapters 1,2,3.
I took the liberty to leave some proofs I considered easy as exercises.

Chapter 0

Introduction

Galois Theory was invented to help study polynomial equations in one variable.

Example. $x^2 + 2x = 3$, *we can solve this by factoring:* $x^2 + 2x - 3 = (x - 1)(x + 3)$, *or use the formula.*

rest of introductory lecture missing...

Chapter 1

Rings and Fields

Definition. *A* ring*, by which we mean a commutative ring with a* 1*, is the following:*

- *A (non-empty) set* R*,*
- *Elements* $0,\ 1 \in R$*,*
- *Maps* $+ : R \times R \to R,\ \times : R \times R \to R$*. For* $r, s \in R$ *we write* $+(r, s) = r + s$ *and* $\times(r, s) = r \times s = r \cdot s = rs$*,*

satisfying the following axioms:

1. $(R, +)$ *is an abelian group with identity* 0*,*
2. $(R, \times)$ *is a commutative semi-group, with identity* 1*, i.e,*
   - $a(bc) = (ab)c \quad \forall a, b, c \in R$*,*
   - $1a = a = a1 \quad \forall a \in R$*,*
   - $ab = ba \quad \forall a, b \in R$*,*
3. $a(b + c) = ab + ac \quad \forall a, b, c \in R$*.*

Example. $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$*,* $\mathbb{C}$ *are all rings.*

Example. ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}} = \{[0], [1], \ldots, [n-1]\}$ *is a ring as well. (Exercise: make sure* $\times$ *makes sense on* ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$*)*

Definition. *A* field *is a ring* R *with the property that* $R \setminus \{0\}$ *is an abelian group under multiplication.*

Remark. *Informally, a field is a place where we can do* $+, -, \times, /$ *as we wish (except for division by zero)*

Example. $\mathbb{Q}$*,* $\mathbb{R}$*,* $\mathbb{C}$ *are all fields,* $\mathbb{Z}$ *however is not (*$2, 3 \in \mathbb{Z}$*,* ${}^{2}\!/_{3} \notin \mathbb{Z}$*).*

Example. *Also if* p *is prime then* ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$ *is a field.*
To show this we need to show that if $1 \leq i \leq p-1$*, then there exists* j*, such that* $ij = 1 + pk$ *for* $k \in \mathbb{Z}$*.*
However $i < p \implies \gcd(i, p) = 1 \implies \exists \lambda, \mu$ *such that* $\lambda i + \mu p = 1$*, so if we pick* $j = \lambda$*, we have a multiplicative inverse for* i*.*

What are the finite fields?

Fact: If $n \in \mathbb{Z}_{\geq 2}$ then there is a field of size n if and only if n is the power of a prime number, and such a field is unique up to isomorphism.

Remark. *So there is a field of size* 9*, but it is not* $\mathbb{Z}/9\mathbb{Z}$*, as* $3 \times 3 = 0$*, but we can not have zero dividers.*
The field of size 9 *is* $(\mathbb{Z}/3\mathbb{Z})[i] = \{a + bi : a, b \in \mathbb{Z}/3\mathbb{Z}\}$ *(this works as there are no solutions to* $x^2 = -1$ *in* $\mathbb{Z}/3\mathbb{Z}$*).*

Proposition 1.1. *Say* K *is a field and* $E \subseteq K$ *is a subset. Then* E *(with induced* $0, 1, +\times$*) is a subfield if and only if*

- $0,\ 1 \in E$
- *If* $a, b \in E$ *then so are* $a + b$*,* $a - b$*,* $a \times b$ *and if* $b \neq 0$ *then* a/b *is too.*

Proof. $\implies$: trivial
$\impliedby$: Check axioms, but they are true in K! □

Example. $\mathbb{Q} \subseteq \mathbb{C}$ *is a subfield: If* $a, b \in \mathbb{Q}$ *then so are* $a + b$*, ...*

Example. *Set* $E = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$*.* $E \subseteq \mathbb{R} \subseteq \mathbb{C}$*, but is* E *a field?*
Let us use 1.1. Set $a = r + s\sqrt{2}$ *and* $b = t + u\sqrt{2}$*,* $r, s, t, u \in \mathbb{Q}$*. So* $a, b \in E$*.*
Obviously $0, 1 \in E$*. So we just need to check* $a \pm b$*,* ab*,* $a/b \in E$*.*

$$a \pm b = \underbrace{(r \pm t)}_{\in\mathbb{Q}} + \underbrace{(s \pm u)}_{\in\mathbb{Q}}\sqrt{2} \in E$$

$$\begin{aligned} ab &= (r + s\sqrt{2})(t + u\sqrt{2}) \\ &= \underbrace{(rt + 2su)}_{\in\mathbb{Q}} + \underbrace{(ru + st)}_{\in\mathbb{Q}}\sqrt{2} \in E \end{aligned}$$

Assume $b \neq 0$

$$\begin{aligned} \frac{a}{b} &= \frac{r + s\sqrt{2}}{t + u\sqrt{2}} \\ &= \frac{r + s\sqrt{2}}{t + u\sqrt{2}} \times \frac{t - u\sqrt{2}}{t - u\sqrt{2}} \\ &= \frac{(rt - 2us) + (st - ru)\sqrt{s}}{t^2 - 2u^2} \end{aligned}$$

$t^2 - 2u^2 = 0$ *implies either* $t = u = 0 = b$*, but we assume* $b \neq 0$ *or* $t/u = \pm\sqrt{2}$*, but* $\sqrt{2}$ *is irrational, so this is impossible as well.*

$$= \frac{(rt - 2us)}{t^2 - 2u^2} + \frac{(st - ru)}{t^2 - 2u^2}\sqrt{s} \in E$$

So $\mathbb{Q}(\sqrt{2})$ *is a field.*

Is $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}$ a field?

It is obviously a ring...
Here is a really important trick:
Say R is a ring and $K \subseteq R$ is a subring such that K is a field. Then R is naturally a vector space over K:
If $\lambda \in K$ and $v \in R$ then $\lambda, v \in R$, therefore $\lambda v \in R$ so K acts on R.
All the other vector space axioms follow immediately from the ring axioms.

Example. *$R = \mathbb{C}$, $K = \mathbb{R}$, $\mathbb{R} \hookrightarrow \mathbb{C}$, therefore $\mathbb{C}$ is a vector space over $\mathbb{R}$, $\dim_{\mathbb{R}} \mathbb{C} = 2$. and a basis is $\{1, i\}$.*

Example. *$\mathbb{Q}(\sqrt{2})$ is a vector space over the subfield $\mathbb{Q}$, $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = 2$, a basis is $\{1, \sqrt{2}\}$.*

Example. *The polynomial ring. $\mathbb{C}[T]$ has elements*

$$\sum_{i=0}^{n} \lambda_i T^i \quad \lambda_i \in \mathbb{C}$$

$\mathbb{C} \subseteq \mathbb{C}[T]$, the polynomials of degree 0, (and the 0 polynomial), so $\mathbb{C}[T]$ is a vector space over $\mathbb{C}$. It is ∞-dimensional, a basis is the set

$$\{1, T, T^2, T^3, \dots\}$$

Proposition 1.2. *Say R is a subring of $\mathbb{C}$, with $\mathbb{Q} \subseteq R \subseteq \mathbb{C}$. Assume furthermore that $\dim_{\mathbb{Q}} R$, the $\mathbb{Q}$-dimension of R considered as a $\mathbb{Q}$ vector space is finite.*
Then R is a field.

Remark. *Hence $\mathbb{Q}(\sqrt[3]{2})$ is a field, $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})) = 3$ and a basis is $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$.*
In particular

$$\frac{1}{1 + \sqrt[3]{2} + 7(\sqrt[3]{2})^2} \in \mathbb{Q}(\sqrt[3]{2})$$

Proof. R is a ring, we need to check that if $0 \neq r \in R$, then $\frac{1}{r} \in R$.
Consider the map $\phi_r : R \to R$, defined by $\phi_r(a) = ra$. (Note R is a ring, so $ra \in R$.)
$\phi_r(a + b) = r(a + b) = ra + rb$, $\forall a, b \in R$ and $\phi_r(\lambda a) = r\lambda a = \lambda ra = \lambda \phi_r(a) \forall \lambda \in \mathbb{Q}, a \in R$.
So ϕ_r is a $\mathbb{Q}$-linear map $R \to R$.
What is $\mathrm{Ker}(\phi_r)$?
It is $\{a \in R : \phi_r(a) = 0\} = \{a \in R : ra = 0\}$. But $r, a \in \mathbb{C}$ and $r \neq 0$ by assumption, so $ra = 0 \implies a = 0$ as $\mathbb{C}$ is a field.
So $\mathrm{Ker}(\phi_r) = \{0\}$. But $\dim_{\mathbb{Q}}(R) = d < \infty$, so by rank-nullity, $\dim(\mathrm{Im}\, \phi_r) = d$ and $\mathrm{Im}(\phi_r) \subseteq R$, so $\mathrm{Im}\, \phi_r = R$, so ϕ is surjective. Hence there exists $s \in R$ such that $\phi_r(s) = rs = 1$, so $\frac{1}{r} = s \in R$. □

Remark. *π is known to be a transcendental number. i.e. if $f(x) \in \mathbb{Q}[x]$ and $f(\pi) = 0$ then f was the zero polynomial.*

Definition. *Let us define*

$$\mathbb{Q}[\pi] = \left\{ \sum_{i=0}^{n} \lambda_i \pi^i : \lambda_i \in \mathbb{Q} \right\}$$

the smallest subring of $\mathbb{C}$ *containing* $\mathbb{Q}$ *and* π*.*

Exercise. *Check:* $\dim_{\mathbb{Q}}(\mathbb{Q}[\pi]) = \infty$ *and that* $\frac{1}{\pi}$ *is not in it.*

Polynomial Rings

Definition. *Let* K *be a field (or even a ring). The polynomial ring* $K[x]$ *is the set of polynomials (of any finite degree) in* x*, with coefficients in* K*. i.e.* $f \in K[x]$ *is of the form*

$$\lambda_0 + \lambda_1 x + \cdots + \lambda_d x^d \quad , \lambda_i \in K.$$

Remark. *If* f *is a polynomial then* f *gives rise to a function* $K \to K$*: send* $\alpha \in K$ *to* $f(\alpha) = \lambda_0 + \lambda_1 \alpha + \cdots + \lambda_d \alpha^d \in K$*. It can happen that different polynomials give the same function:*
If $K = \mathbb{Z}/2\mathbb{Z}$*, let* $f(x) = x$ *and* $g(x) = x^2$*, then* $f \neq g$*, but* $f(x) = g(x) \forall x \in K$*. (However this only happens in finite fields)*

Definition. *Say* $f = \lambda_0 + \lambda_1 x + \cdots + \lambda_d x^d$*, with* $\lambda_d \neq 0$*. We say the* degree *of* f*,* $\deg(f)$*, is* f*. The* leading coefficient *is* λ_d*, the* leading term *is* $\lambda_d x^d$ *and the* constant coefficient *is* λ_0*. We say* f *is* monic *if* $\lambda_d = 1$*.*

The polynomial 0 is a special case: Sometimes it is helpful to define $\deg(0) = -1$ or $\deg(0) = -\infty$. For the point of this course (or these lecture notes) we will leave $\deg(0)$ undefined.

Addition and Multiplication of polynomials

If $f = \sum_{i=0}^{m} \lambda_i x^i$ and $g = \sum_{i=0}^{n} \mu_i x^i$, WLOG $m \leq n$, then expand the set of λ_i, $0 \leq i \leq m$ to λ_i, $0 \leq i \leq n$, by setting $\lambda_i = 0$, $\forall m < i \leq n$.
Now $f = \sum_{i=0}^{n} \lambda_i x^i$.
Define

$$f + g = \sum_{i=0}^{n} (\lambda_i + \mu_i) x^i$$

$$f - g = \sum_{i=0}^{n} (\lambda_i - \mu_i) x^i$$

$$fg = \sum_{i=0}^{m+n} \gamma_i x^i$$

where

$$\gamma_i = \sum_{i=0}^{k} \lambda_i \mu_{k-i}$$

Exercise: Check this makes $K[x]$ into a ring.

Remark. *Note that $K \subseteq K[x]$ and hence $K[x]$ is a vector space over K, if K is a field.*

Proposition 1.3. *If f and g are polynomials in $K[x]$, (K a field) and $g \neq 0$ then there exists polynomials q and r, such that*

1. $f = gq + r$
2. $\deg(r) < \deg(g)$

Furthermore, g and r are unique.

Example. *Say $K = \mathbb{C}$, $f = x^3 - x^2$, $g = x^2 + 1$.*
Then (long division or any other method) $f = (x-1)g + (-x+1)$.

Proof. We have done this in literally every course I attended this year. I won't type it down again. □

Remark. *Now that we have Euclid's algorithm uniqueness of prime factorization follows immediately.*

Definition. *Say f, $g \in K[x]$, K a field and f and g not both zero. The highest common factor $h(x) =$* hcf *of f and g is a polynomial h such that*

1. *h divides f and h divides g.*
2. *If j is any polynomial such that j divides f and j divides g, then j divides h.*

Proposition 1.4. *If at least one of f and g is non-zero, then a highest common factor exists. Furthermore, if h_1 and h_2 are highest common factors of f and g then there exists $\lambda \in K$, $\lambda \neq 0$ such that $\lambda h_1 = h_2$.*

Proof. Again, done so many times in previous courses. □

Corollary 1.5. *Say f, $g \in K[x]$ at least one non-zero and if h is an* hcf *of f and g, then there exists polynomials $\lambda, \mu \in K[x]$ such that $h = \lambda f + \mu g$.*

Proof. Go backwards in the proof for 1.4 □

Irreducible Polynomials

Definition. *Say K is a field, $f \in K[x]$. We say f is* irreducible *if*

1. $f \neq 0$
2. $\deg f > 0$
3. *If $f = gh$, with $g, h \in K[x]$, then either* $\deg(g) = 0$ *or* $\deg(h) = 0$

Remark. *If $K = \mathbb{C}$ then $f \in K[x]$ irreducible is equivalent to* $\deg(f) = 1$.

Example. *If $K = \mathbb{R}$ then $x^2 + 1$ is irreducible.*
If $K = \mathbb{Q}$, is $x^4 - 2$ irreducible? Is $x^4 + 4$ irreducible?

Theorem 1.6. *Say $f \neq 0$, $f \in K[x]$. Then*

1. *$f = up_1p_2p_3 \dots p_n$, $u \in K$, $u \neq 0$ with all the p_i irreducible polynomials in $K[x]$.*
2. *If $f = vq_1q_2q_3 \dots q_m$, with $v \in K$, $v \neq 0$ and all the q_j irreducible polynomials in $K[x]$. Then $n = m$ and after reordering the q_i if necessary $q_i = \lambda_i p_i$, $\lambda_i \in K$, $\lambda_i \neq 0$ $\forall i$.*

Proof. Only a sketch of a proof was given. □

Let us talk about irreducible polynomials.
By the Fundamental Theorem of Algebra, if $p(x) \in \mathbb{C}[x]$ of degree ≥ 1, then there exists $\lambda \in \mathbb{C}$ such that $p(\lambda) = 0$, hence $p(x) = (x - \lambda)q(x)$. So if p has degree strictly bigger than 1, we have just factored it.
Conclusion: Any polynomials $p(x) \in \mathbb{C}[x]$ of degree > 1 is reducible. Now it is easy to check

Proposition. *$p(x) \in \mathbb{C}[x]$ is irreducible if and only if* $\deg p(x) = 1$.

$\mathbb{C}$ is special though, every non-constant polynomial has a root. ($\mathbb{C}$ is algebraically closed.)
K algebraically closed $\implies$ irreducible polynomials in $K[x]$ are the degree 1 polynomials.

Example. *$x^2 + 1$ is irreducible in $\mathbb{R}[x]$. More generally, if $f(x) \in K[x]$ has degree 2, then either $f(x)$ is ireducible or it factors as $u(x - a)(x - b)$ into two linear factors, $a, b, u \in K$.*

Therefore, for a degree 2 polynomial it holds: f is irreducible in $K[x]$ if and only if f has no root in K.
The same trick works for degree 3:
If $f = gh$, a non trivial factorisation, then one of g, h is degree 1, therefore f has a root in K.

Example. *Say $K = \mathbb{Q}$, Say $f(x) = x^3 - 2$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*
Why? if it factored it would have a root in $K = \mathbb{Q}$, but the three complex roots of $x^3 - 2$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$, with $\omega = \mathrm{e}^{2\pi i/3}$.
$\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$ are not even real, let alone rational and $\sqrt[3]{2} \notin \mathbb{Q}$ either.

In degree 4 or more the trouble starts.

Example. *$f(x) = x^4 + 2x^2 + 1 = (x^2+1)^2$. Then f is reducible in $\mathbb{R}[x]$, but $f(\lambda) > 0$ for all $\lambda \in \mathbb{R}$ and in particular $f(\lambda) \neq 0$, so there are no roots in $\mathbb{R}$.*

Example. *What about $x^4 - 2$ (over $\mathbb{Q}$)?*
It has no roots in $\mathbb{Q}$, but does it factor into two quadratics?
Say $x^4 - 2 = (x^2 + ax + b)(x^2 + cx + d)$, $a, b, c, d \in \mathbb{Q}$.
Multiplying out and comparing coefficients gives four non-linear equations in four variables...good luck.

Example. *What about $x^4 + 4$ in $\mathbb{Q}[x]$? It has no roots in $\mathbb{Q}$, but it turns out it is actually reducible.*

Over $\mathbb{Q}$ it turns out $x^n - 2$ is irreducible for all $n \geq 1$. We will now see how to prove this.

Remark. *If a field is finite we can just try all possible factors. For example in $\mathbb{F}_2$, x^2+x+1 is irreducible since $x - 1$ and x do not divide it.*

Say $p(x) \in \mathbb{Q}[x]$. How do we tell if it has a root in $\mathbb{Q}$? Replace p by Np, where $N =$ lcm(denominators of coefficients). So with out loss of generality $p(x) = a_n x^n + \cdots + a_0$, $a_i \in \mathbb{Z}$, $a_n \neq 0$.
Say $\lambda = {}^r\!/_s$ is a root with ${}^r\!/_s \in \mathbb{Q}$ in lowest terms, i.e. $\mathrm{hcf}(r, s) = 1$.
Then

$$p(\lambda) = 0 \implies 0 = a_n \left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1 \frac{r}{s} + a_0$$

multiplying by s^n, we get

$$0 = a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_1 r s^{n-1} + a_n s^n \qquad = a_n r^n + s \cdot (\dots)$$

Since $s \mid 0$, we must have $s \mid a_n r^n$, but $\mathrm{hcf}(r, s) = 1$ so $s \mid a_n$.
Similarly we have $r \mid a_0$.
Now we have finitely many possibilities for s and r.

Remark. *Do not forget signs when looking for solutions.*

What about degree larger or equal than 4?

We will not give a general answer, we will just list a few strategies.

Proposition 1.7 (Gauss' Lemma)**.** *Say $f \in \mathbb{Q}[x]$ and all coefficients are integers. Say $f = gh$, $g, h \in \mathbb{Q}[x]$ of degree $m = \deg(g)$, $n = \deg(h)$.*
Then there exist g' and h', such that $f = g'h'$ and $\deg(g') = m$ and $\deg(h') = n$ and g' and h' have integer coefficients too.

Proof. We know $f = gh$. Now choose $N, M \in \mathbb{Z}_{\geq 1}$ such that $Mg, Nh \in \mathbb{Z}[x]$.
Set $R = MN$. Now $Rf = (Mg)(Nh)$, if $R = 1$, we are done.
If $R > 1$, choose a prime factor $p \mid R$. We will show that either p divides all coefficients of Mg or all coefficients of Nh. We can then proceed by induction on the number of prime

factors.
Write

$$G = Mg \in \mathbb{Z}[x]$$
$$H = Nh \in \mathbb{Z}[x]$$

We know that $GH = Rf$, polynomials whose coefficients are multiples of p since $f \in \mathbb{Z}[x]$.
Assume for a contradiction that both G and H have at least one coefficient that is not a multiple of p.
Say $G = \sum s_i x^i$, $H = \sum t_j x^j$.
Now choose the highest i such that $p \nmid s_i$ and highest j such that $p \nmid t_j$. So

$$G = s_0 + s_1 x + \cdots + \underbrace{s_i}_{p \nmid s_i} x^i + \underbrace{s_{i+1}x^{i+1} + s_{i+2}x^{i+2} + \ldots}_{p \mid s_{i+1},\quad p \mid s_{i+2},\ldots}$$
$$H = t_0 + t_1 x + \cdots + \underbrace{t_j}_{p \nmid t_j} x^j + \underbrace{t_{j+1}x^{j+1} + t_{j+2}x^{j+2} + \ldots}_{p \mid t_{j+1},\quad p \mid t_{j+2},\ldots}$$

Now, what is the coefficient of x^{i+j} in $GH = Rf$? It is

$$\underbrace{\cdots + s_{i-2}t_{j+2} + s_{i-1}t_{j+1}}_{p \mid t_k} + \underbrace{s_i t_j}_{p \nmid s_i t_j} + \underbrace{s_{i+1}t_{j-1} + s_{i+2}t_{j-2} + dots}_{p \mid s_k}$$

So p divides all terms but $s_i t_j$, so p does not divide the sum. But all coeffecients in Rf are multiples of p, so we have a contradiction.
Hence one of G, H can be divided by p.

□

Remark. *A significantly shorter proof: Say $GH \equiv 0 \mod p$ in $(\mathbb{Z}/p\mathbb{Z})[x]$, it is a fact that $(\mathbb{Z}/p\mathbb{Z})[x]$ is an integral domain, so either $G \equiv 0 \mod p$ or $H \equiv 0 \mod p$.*

Corollary 1.8 (Eisenstein's Criterion)**.** *Say $f \in \mathbb{Q}[x]$, $f = \sum_{i=0}^{d} a_i x^i$, $d \geq 1$, and assume*

1. *$a_i \in \mathbb{Z}$, for all i.*
2. *$\exists p$, prime such that $p \nmid a_d$, $p \mid a_i$ for $0 \leq i < d$ and $p^2 \nmid a_0$.*

Then f is irreducible.

Example. *$x^{100} - 2$ is irreducible in $\mathbb{Q}[x]$, using $p = 2$.*
$x^5 + 4x + 2$ is irreducible in $\mathbb{Q}[x]$, using $p = 2$ as well.

Proof. Say $f = gh$, $\deg(g), \deg(h) > 0$, $gh \in \mathbb{Q}[x]$, where f satisfies the above conditions.
So $f \in \mathbb{Z}[x]$, hence by Gauss' Lemma WLOG, $g, h \in \mathbb{Z}[x]$.
Say $g = \sum_{i=0}^{m} s_i x^i$, $h = \sum_{j=0}^{n} t_j x^j$. $s_i, t_j \in \mathbb{Z}$, so $m + n = d$, $s_m t_n = a_d$.
So s_m, t_n are not multiples of p.

Let us choose i and j as low as possible such that $p \nmid s_i$ and $p \nmid t_j$ (such i and j exist as we have just shown). Then the coefficient of x^{i+j} in gh is

$$\cdots + s_{i-1}t_{j+1} + s_i t_j + s_{i+1}t_{j-1} + \dots$$

Now $p \mid s_{i-k}$, for all $k \geq 1$, so $p \mid s_{i-k}t_{j+k}$, and since $p \mid t_{j-k}$ for all $k \geq 1$, $p \mid s_{i+k}t_{j-k}$. But $p \nmid s_i t_j$, therefore the coefficient of x^{i+j} in f is coprime to p.
But $p \mid a_k$, for all $0 \leq k < d$, therefore $i + j = d = m + n$. Hence $i = m$, $j = n$.
In particular $i, j > 0$. Therefore the constant term of f is a multiple of p^2, which is a contradiction since $p^2 \nmid a_0$ by assumption. □

Remark. *$p \nmid a_d$, $p \mid a_k$, for $0 \leq k < d$, so $f \equiv a_d x^d \mod p$, so $(g \mod p)(h \mod p) = a_d x^d$, thus $g \mod p$, $h \mod p$ are monomials too. Hence $p^2 \mid a_0$.*

Corollary 1.9. *If p is a prime number, then the polynomial $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible in $\mathbb{Q}[x]$.*

Proof. We know

$$1 + x + x^2 + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}$$

Set $y = x - 1$, so $x = y + 1$, then

$$\begin{aligned} &= \frac{(y+1)^p - 1}{y} \\ &= \frac{y^p + \binom{p}{1}y^{p-1} + \binom{p}{2}y^{p-2} \cdots + py + 1 - 1}{y} \\ &= y^{p-1} + \binom{p}{1}y^{p-2} + \cdots + \binom{p}{i}y^{p-i-1} + \cdots + p \end{aligned}$$

Now we can apply Eisenstein since $a_{p-1} = 1$, and $p \mid \binom{p}{i}$ for all $1 \leq 1 < p$, so $p \mid a_k$, for $0 \leq k < p - 1$. Finally $p^2 \nmid a_0$.
So Eisenstein applies, hence $1 + x + \cdots + x^{p-1}$ is irreducible. □

Exercise. *If $p > 1$ is not prime, prove that $1 + x + \cdots + x^{p-1}$ is reducible.*

Chapter 2

Field Extensions

i.e. $K \subseteq L$, L and K fields, then L is an extension of K, K is a subfield of L.
Given a big field F, what do all the subfields look like?
This is a "wild" question, so here is an easy fact

Lemma 2.1. *Let F be field and say I is a set and for each $i \in I$, say $E_i \subseteq F$ is a subfield, then*

$$\bigcap_{i \in I} E_i$$

is a subfield of F.

Proof. Set $E = \bigcap_{i=I} E_i$.

Recall. *$X \subseteq F$ is a subfield if and only if $0, 1 \in X$ and if $x, y \in X$ then so are $x+y$, $x-y$, xy and x/y(if $y \neq 0$)*

Now it is easy to see that $0,\ 1 \in E_i\ \forall i \in I$, so $0,\ 1 \in E$.
Similarly, if $x, y \in E$, that means that $x, y \in E_i\ \forall i$. So $x+y$, $x-y$, xy and x/y(if $y \neq 0$) are $\in E_i\ \forall i$, hence they are in E. □

As a consequence, given a field F, we can look at he intersection of *all* the subfields of F.
This is called the *prime subfield*, or the *primefield* of F.
By Lemma 2.1 it is the smallest subfield of F.
What does it look like?

Example. *$F = \mathbb{C}$ Any subfield will contain 0 and 1, if x, y are in F, then $x+y$ is in F as well, so every subfield must contain $\mathbb{Z}$.*
Similarly every x/y must be contained, so $\mathbb{Q}$ is a subset of every subfield of $\mathbb{C}$.
Conversely $\mathbb{Q}$ is a subfield of $\mathbb{C}$, so the prime subfield of $\mathbb{C}$ is $\mathbb{Q}$.

General Case

Say F is any field. If $E \subseteq F$ is any subfield then $0, 1 \in E$.
We can get a map $\mathbb{Z} \to E$, $n \to (1 + 1 + \cdots + 1)$, if $n > 0$ and the additive inverse of $-n$ if $n < 0$. Now there are two very distinct cases:

1. $\mathbb{Z} \to E$ is injective. Then E contains a copy of $\mathbb{Z}$. But E is a field, so E contains a copy of $\mathbb{Q}$, which is necessarily the prime subfield.

2. $\mathbb{Z} \to E$ is not injective. Then $\mathbb{Z} \to E$ is a group homomorphism, so the Kernel must be of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}_{\geq 1}$ (For a proof look at the smallest positive element of the kernel) and by the first isomorphism theorem we have an injection $\mathbb{Z}/n\mathbb{Z} \to E$. What can we say about n?
   First of all we can say that $n \neq 1$. If $n = 1$, we have $0 = 1$ and $E = \{0\}$, which is not a field.
   Secondly, if n is not prime, we can write $n = ab$, $1 < a, b < n$. In E, $a \neq 0$, $b \neq 0$, but $ab = n = 0$, which can not happen in a field.
   Therefore n is prime and $E \supseteq {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, which is a field and therefore the prime subfield of E;

In Case 1, $\mathbb{Q} \subseteq F$, we say F has characteristic 0. In Case 2, we say F has characteristic p.

Remark. *If F has characteristic p the $\forall x \in F$, $x + x + x + x + \cdots + x$ (p times) $= 0$.*

Now say $K \subseteq L$ are fields. Say $a \in L$ (interesting case $a \notin K$). What is the smallest subfield of L containing K and a? Does that question even make sense?
Let us consider all subfields of L containing K and a. By 2.1 their intersection is a field as well, contains K and a and it is the smallest such field.
Let us call it $K(a)$.

Definition. *$K(a)$ is the smallest subfield of L containing K and a.*

Definition. *More generally, say $a_1, \ldots, a_n \in L$ and $K \subseteq L$ is a subfield of L. Then*

$$K(a_1, \ldots, a_n)$$

Is the smallest subfield of L containing K and $a_1, \ldots, a_n$. (i.e. the intersection of all such fields)

Remark. *If $S \subseteq L$ is any subset, we can define $K(S)$ similarly.*

Example. $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$, *what is this?*
Say $E \subseteq \mathbb{C}$ is any subfield, and $E \supseteq \mathbb{Q}$ and $E \ni \sqrt{2}$. Then E must contain ant number of the form $a + b\sqrt{2}$, $a, b \in \mathbb{Q}$. However $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a field, so it must be $\mathbb{Q}(\sqrt{2})$.

Example. *Similarly $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 : a, b, c \in \mathbb{Q}\}$ (All these numbers must be contained, and it is a field by 1.2)*

Example. $\mathbb{Q}(\sqrt{2},\sqrt{3}) = ?$
Any subfield of $\mathbb{C}$ *containing* $\mathbb{Q}$, $\sqrt{2}$ *and* $\sqrt{3}$ *must firstly contain* $\sqrt{2}\sqrt{3} = \sqrt{6}$ *and hence must contain*

$$\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$$

Now check this is a ring. This is true, because if $x, y \in \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ *then* $x, y \in E$.
By 1.2 this is a field $\mathbb{Q}(\sqrt{2}\sqrt{3})$.

Example. *What is* $\mathbb{Q}(\pi)$. *Fact* $\nexists p \in \mathbb{Q}[x]$ *such that* $p \neq 0$ *but* $p(\pi) = 0$ *(Lindemann)*
Say $\mathbb{Q}(\pi) = E$. $\pi \in E$. *So therefore* $E \ni \pi^2, \pi^3, \dots$.

Claim. *The set* $\{1, \pi, \pi^2, \dots\}$ *is a linearly independent set of vectors in the* $\mathbb{Q}$*-vector space* E.

Proof. A non-trivial combination implies a counter example to Lindemann. □

Notation. $\mathbb{Q}[\pi] = \{p(\pi) : p \in \mathbb{Q}[x]\}$, *polynomials in* π *with rational coefficients*

$\mathbb{Q}[\pi]$ *is a ring* $\mathbb{Q}[\pi] \cong \mathbb{Q}[x]$, $\dim_{\mathbb{Q}} \mathbb{Q}[\pi] = \infty$. *So we cannot apply 1.2 to deduce* $\mathbb{Q}[x]$ *is a field and indeed* $\mathbb{Q}[x]$ *is* not *a field.*
Division is the issue: If $f(x) \in \mathbb{Q}[x]$, $g(x) \in \mathbb{Q}[x]$ *and* $g \neq 0$ *and* g/f *(in* $\mathbb{Q}[\pi]$*) then* $\frac{f(\pi)}{g(\pi)} \in \mathbb{Q}[\pi]$. *But if* $g \nmid f$ *it won't be in* $\mathbb{Q}[\pi]$. *In fact,*

$$\mathbb{Q}[\pi] = \left\{ \frac{f(\pi)}{g(\pi)} : f, g \in \mathbb{Q}[x], g \neq 0 \right\}$$

as $\mathbb{Q}(\pi)$ *clearly contains all* $f(\pi)/g(\pi)$ *and conversely that is easily checked to be a field*

Definition. *(Notation* $K \subseteq L$*, both fields)We say an element* $a \in L$ *is algebraic over* K *if* $\exists$ *a polynomial* $p(x) \in K[x]$ *such that* $p \neq 0$ *but* $p(a) = 0$.
If $a \in L$ *is not algebraic over* K*, we say it is transcendental over* K.

Remark. *If* $K = \mathbb{Q}$ *and* $L = \mathbb{C}$ *we usually just say* $a \in \mathbb{C}$ *is algebraic or transcendental.*

Example. $\sqrt{2}$ *is algebraic over* $\mathbb{Q}$. $p(x) = x^2 - 2$.

Example. π *is not algebraic over* $\mathbb{Q}$. *(Lindemann)*

Remark. *However,* π *is algebraic over* $\mathbb{R}$*:*

$$p(x) = x - \pi \in \mathbb{R}[x]$$

even $i\pi$ *is algebraic over* $\mathbb{R}$*:* $(x) = x^2 + \pi^2 \in \mathbb{R}[x]$

Example. *Are there any $z \in \mathbb{C}$ not algebraic over $\mathbb{R}$? No*

$$(x - z)(x - \bar{z}) = x^2 - (z + \bar{z})x + (z\bar{z})$$

So all complex numbers are algebraic over $\mathbb{R}$.

Definition. *$K \subseteq L$, we say L is algebraic over K if all $a \in L$ are algebraic over K. (e.g. $\mathbb{C}$ is algebraic in $\mathbb{R}$, but $\mathbb{R}$ is not algebraic over $\mathbb{Q}$)*

Remark. *in fact, only countably many real numbers are algebraic over $\mathbb{Q}$. Therefore* 100% *of real numbers are not algebraic over $\mathbb{Q}$.*

Definition. *Say $K \subseteq L$ are fields and $a \in L$ is algebraic over K. We say the* minimum polynomial of a over K *is the non-zero polynomial $p(x) \in K[x]$ such that*

1. *$p(a) = 0$,*
2. *p is monic,*
3. *p is irreducible over K.*

Proposition 2.2. *If $a \in L$ is algebraic over K, then there exists a minimum polynomial for a over K. This polynomial is unique and furthermore if $p(x)$ is the minimum polynomial of a and $f(x) \in K[x]$ is any polynomial, then $f(a) = 0$ if and only if $p(x)$ divides $f(x)$ in $K[x]$*

Proof. Set $S = \{f(x) \in K[x] : f(a) = 0, f \neq 0\}$. $a \in L$ is algebraic over K, means that S is non-empty. Therefore there exists a polynomial $q(x)$ of smallest degree.

$$q(x) = \lambda_d x^d + \dots$$

Set

$$p(x) = \frac{1}{\lambda_d} q(x)$$

So $p(x)$ is monic, and $p(a) = {}^1\!/_{\lambda_d} q(a) = {}^1\!/_{\lambda_d} 0 = 0$.

Claim. *$p(x)$ is irreducible in $K[x]$.*

Well $p(x) \not\equiv 0$ and $p(a) = 0$, so $p(x)$ is not constant. Say $p(x) = f(x)g(x)$, $\deg(f), \deg(g) > 0$.
Note that $\deg(p) = \deg(f) + \deg(g)$, so $\deg(f), \deg(g) < \deg(p)$.
Moreover $p(a) = 0$, so $f(a)g(a) = 0$, hence one of $f(a)$ and $g(a) = 0$.
With out loss of generality $f(a) = 0$, so $f \in S$, but p is smallest degree in S, so we have reached a contradiction.
Hence p is irreducible. So existence is done.
Now say $f \in K[x]$. We can write $f(x) = q(x)p(x) + r(x)$, $\deg(r) < \deg(p)$. If $f(a) = 0$, then evaluating the right side for $x = a$, we get $0 = q(a)p(a) + r(a) = r(a)$, since $p(a) = 0$. So $r(a) = 0$, but again, p is the polynomial of minimal degree, with a as a root, therefore $r \equiv x$.
Hence $p \mid f$.
Conversely if $p \mid f$ and $p(a) = 0$, then $f(a) = 0$.
Uniqueness: If p_1 and p_2 are both minimal polynomials then $p_1 \mid p_2$ and $p_2 \mid p_1$, but since they are both monic this means $p_1 = p_2$. □

Corollary. *A consequence of this is the following: $K \subseteq L$, $a \in L$ algebraic over K. Let $p(x) \in K[x]$ be the minimum polynomial of a over K and say $p(x)$ has degree $d > 1$. Then any element of L which can be expressed as a polynomial in a with coefficients in K can also be written as a polynomial in a with coefficients in K and of degree $< d$.*

Example. *$K = \mathbb{R}$, $L = \mathbb{C}$, $a = i$, $p(x) = x^2 + 1$, $d = 2$. The claim is that $53i^9 + 27\frac{12}{den}i^3 - \pi i + \sqrt{2}$ is of the form $x + iy$, $x, y \in \mathbb{R}$.*

Proof. If the element of L is $f(a)$, $f(x) \in K[x]$, then write $f(x) = q(x)p(x) + r(x)$. By 1.3 $\deg(r) < d$ and sub in a to get $f(a) = 0 + r(a)$, because $P(a) = 0$. □

Proposition 2.3. *$K \subseteq L$, fields, $a \in L$.*

(a) If a is algebraic over K then the field $K(a) \subseteq L$ is finite-dimensional, as a K-vector space and moreover $\dim_K K(a)$ is the degree of the minimal polynomial of a over K.

(b) If a is transcendental over K, then $K(a)$ is an infinite dimensional extension as a K-vector space.

Proof.

(a) Say $p(x)$ is the minimal polynomial of a, with degree ≥ 1. Let R be the K-vector subspace of L spanned by a^i, $0 \leq i < d$. Clearly $\dim_K R \leq d$. In fact $\dim_K R = d$, because any non-trivial linear combination of the a^i is not zero, because a is not a root of a polynomial in $K[x]$ of degree less than d.

Claim. $R = K(a)$.

Well, clearly $R \subseteq K(a)$. It suffices to show that R is a field. 0, 1, +, − are trivial.
Is R closed under multiplication and division?
$R = \{f(a) : f \in K[x], \deg(f) < d\}$. If $f(a)$ and $g(a) \in R$, then $f(a)g(a)$ is some polynomial in a, therefore by the previous corollary it is equal to a polynomial in a of degree $< d$, so it is in R.
So R is a ring, $\subseteq L$ a field, $\dim_K R < \infty$ so by 1.2 and the remark after it R is a field.

(b) If $a \in L$ is not algebraic over K then $K(a) \supseteq \{1, a, a^2, \dots\}$ an infinite linearly independent subset, therefore $\dim_K K(a) = \infty$.

□

Definition. *$K \subseteq L$, $a \in L$ algebraic over K. The degree of a over K, is the degree of the minimal polynomial of a over K.*

Example. *$K = \mathbb{Q}$, $L = \mathbb{C}$, $a = \sqrt[100]{7}$, what can we prove about $K(a)$?*

Claim.

$$\mathbb{Q}(a) = \left\{ \sum_{i=0}^{99} \lambda_i a^i : \lambda_i \in \mathbb{Q} \right\}$$

and $\{a^i : 0 \leq i \leq 99\}$ are a basis for a 100-dimensional $\mathbb{Q}$-vector space $\mathbb{Q}(a)$.

Here is why:
Clearly $a^{100} = 7$, therefore a is a root of $p(x) = x^{100} - 7 \in \mathbb{Q}[x]$, $p(x)$ is irreducible by Eisenstein.
So the degree of a over $\mathbb{Q}$ is 100 and $a^i : 0 \leq i \leq 99$ are linearly independent over $\mathbb{Q}$, by 2.3(a) and its proof.
Also by 2.3(a), $\mathbb{Q}(a)$ is spanned by $\{a^i\}_{i=0}^{99}$, so it is what we claimed.

Example. *$K = \mathbb{Q}$, $L = \mathbb{C}$,$a = \varsigma_p = e^{2\pi i/p}$, p prime.*
What is the dimension of $\mathbb{Q}(\varsigma_p)$?
Clearly a is algebraic over $\mathbb{Q}$, because $a^p = 1$, therefore a is a root of $x^p - 1$. However

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1) \in \mathbb{Q}[x]$$

which are both irreducible in $\mathbb{Q}[x]$, by linearity and Eisenstein-corollary respectively.
Which is the minimal polynomial of ς_p? ς_p must be a root of the irreducible polynomial, since $\varsigma_p \neq 1$, the minimal polynomial is $x^{p-1} + x^{p-2} + \cdots + x + 1$.
Therefore the degree of ς_p over $\mathbb{Q}$ is $p-1$, so $\dim_{\mathbb{Q}} \mathbb{Q}(\varsigma_p) = p - 1$, because $x^{p-1} = -(x^{p-2} + \cdots + x + 1)$, so a $\mathbb{Q}$-basis for $\mathbb{Q}(\varsigma_p)$ is $\{1, \varsigma_p \ldots, \varsigma_p^{p-2}\}$

Up until now, our set-up has been $K \subseteq L$, $a \in L$, algebraic over K, $p(a)$ is the minimal polynomial of a, $p(x) \in K[x]$, irreducible and $p(x)$ has a root in L.
Now let us forget about L and say that all we have is a field K and an irreducible $p(x) \in K[x]$. Can we build $K(a)$, a a root of $p(x)$ in any meaningful way?

Example.

1. $K = \mathbb{R}$, $p(x) = x^2 + 1$
2. $K = {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$, $p(x) = x^2 - 2$.

Idea (inspired by $\mathbb{R} \subseteq \mathbb{C}$ and the above arguments): Set $R = \{f(x) \in K[x] : \deg(f) < d\}$, where $d = \deg(p)$. $\dim_K R = d$, a basis is $1, x, \ldots, x^{d-1}$.
Addition and subtraction are ok, and we can redefine multiplication as follows (similar to before): $f(x) \times g(x)$ may have degree $\geq d$, then we write $f(x)g(x) = q(x)p(x) + r(x)$, with $\deg(r) < d$, so $r(x) \in R$, and define $f(x) \times g(x) = r(x)$.

Remark. *This looks a bit like ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$: e.g. ${}^{\mathbb{Z}}\!/_{10\mathbb{Z}} = \{0, 1, \ldots, 9\}$ and $6 \times 7 = 42 \geq 10$, so $6 \times 7 = 2$ in ${}^{\mathbb{Z}}\!/_{10\mathbb{Z}}$, because the remainder is 2.*

Theorem 2.4 (Construction)**.** *Say K a field, $p(x) \in K[x]$ an irreducible polynomial, degree $d \geq 1$. Let I be the subgroup of $K[x]$, consisting of multiples of $p(x)$. ($K[x]$ is an abelian group, with I some subgroup)*
Consider the quotient group $M = {}^{K[x]}\!/_{(p)}$. Then M is naturally a field, containing (a copy of) K, and M contains a root α of $p(x)$ (namely $\alpha = x + I$).
The K-dimension of M is d (the degree of $p(x)$).
Furthermore, M has the following "universal property": If L is any field containing K and $a \in L$ is any root of $p(x)$ in L, then there exists an isomorphism of fields $M \to K(a)$, which is the identity on K and sends α to a.

Proof. M is an abelian group. There is a map $K \to M$ ($K \hookrightarrow K[x] \to {}^{K[x]}/_{(p)}$=M), so let us define $1 \in M$ to be the image of 1 in K.
Next let us define a multiplication on M:
Given m_1, $m_2 \in M$, lift them to f_1,$f_2 \in K[x]$. Define $m_1 \times m_2$ as the image of $f_1 \times f_2$ under the map $K[x] \to M$.
But is this well-defined? Yes, if g_1 and g_2 are different lifts (pre-images), then $g_1 - f_1$ and $g_2 - f_2$ are multiples of $p(x)$, then

$$\begin{aligned} g_1g_2 - f_1f_2 &= g_1g_2 - g_1f_1 + g_1f_2 - f_1f_2 \\ &= g_1(g_2 - f_2) + (g_1 - f_1)f_2 \end{aligned}$$

which is a multiple of $p(x)$, so the images of g_1g_2 and f_1f_2 coincide.
Now M is a ring, because it inherits the axioms from $K[x]$.
Note also: an element of M is a subset $f + I$ of $K[x]$.
If $f = qp + r$ with $\deg(r) < d$, then $r \in f + I$ and (easy to check)r is the only element of $f + I$ with degree $< d$. Therefore as a set $M \cong \{$polynomials in $K[x]$ of degree $< d\}$.
This is an isomorphism of groups and of K-vector spaces, therefore $\dim_K M = d$ and a basis is

$$1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{d-1}$$

M is a field, say $0 \neq m \in M$. Lift m to $f \in K[x]$, f not a multiple of $p(x)$. But $p(x)$ is irreducible, therefore $\mathrm{hcf}(f, p) = 1$.

Remark. *This is the first time we assume $p(x)$ is irreducible*

Therefore there exists $\lambda, \mu \in K[x]$ such that $\lambda f + \mu p = 1$. (Cor 1.5) Set $n = \lambda + I \in M$, Then

$$\begin{aligned} mn &= \lambda f + I \\ &= \lambda f + \mu p + I \\ &= 1 + I \end{aligned}$$

Example. ${}^{\mathbb{R}[x]}/_{(x^2+1)} \cong \mathbb{C}$ *(where $(x^2 + 1)$ is all the multiples of $x^2 + 1$).*

Set $\alpha = x + I \in M$, then $p(\alpha) = p(x) + I = I = 0 + I$, so α is a root of $p(x) \in M$.
Finally, universal property, say $K \subseteq L$ and $a \in L$ is a root of $p(x)$.
Define $\varphi : K[x] \to L$, a ring homomorphism, defined by $\varphi(f(x)) = f(a)$, φ is a group homomorphism and even a ring homomorphism.
By the first isomorphism theorem ${K[x]}/{}_{p\mathbb{Z}}\,\mathrm{Ker}(\phi) \cong \mathrm{Im}\,\varphi$.

$$\begin{aligned} \mathrm{Ker}(\varphi) &= \{f(x) \in K[x] : f(a) = 0\} \\ &= \text{multiples of } p(x) \end{aligned}$$

by 2.2

$$= I$$

Therefore we get an induced map $M \overset{\varphi}{\hookrightarrow} L$, and $M \cong \{f \in K[x] : \deg f < d\}$, therefore $\mathrm{Im}\,\varphi = \{$polynomials in a, coefficients in K, degree smaller $d\} = K(a)$, by 2.3 □

Example. *q odd, prime and $p(x) = x^2 - n$, where $0 < n < q$ is a quadratic non-residue, $p(x)$ irreducible, $M = (\mathbb{Z}/q\mathbb{Z})[x]/(\text{multiples of } p)$, a field of dimension 2 over $\mathbb{Z}/q\mathbb{Z}$, therefore a field of size q^2*

We now have a trick:
Given K a field and $p(x) \in K[x]$ a irreducible polynomial, we can build a bigger field M where p has at least one root.
We can repeat this procedure and throw in more roots, so we should better be able to control what happens if we have towers of fields, e.g. $K \subseteq L \subseteq M$.

Example. *not sure where to put this example...*
$K = \mathbb{Q}$, $p(x) = x^3 - 2$, $M = \mathbb{Q}[x]/((\text{multiples of } x^3 - 2) = I)$, and if $\alpha = x + I$, then $\dim_{\mathbb{Q}} M = 3$ and a basis is $1, \alpha, \alpha^2$.

Example. *$L = \mathbb{C}$ and let a, b, c be three roots of $p(x)$ $a = \sqrt[3]{2} \in \mathbb{R}$, $b = \omega a$, $c = \omega^2 a$. Now $\mathbb{Q} \subset \mathbb{Q}(a), \mathbb{Q}(b), \mathbb{Q}(c) \subset \mathbb{C}$. $\mathbb{Q}(a), \mathbb{Q}(b), \mathbb{Q}(c)$ are all fields obtained by throwing in a root of $p(x)$ into $\mathbb{Q}$.*
Note $a \in \mathbb{R}$ and therefore $\mathbb{Q} \subset \mathbb{R}$, but $b \notin \mathbb{R}$, therefore $\mathbb{Q}(b) \neq \mathbb{Q}(a)$.
However, both are isomorphic to M (by 2.4), and therefore isomorphic *to each other $\mathbb{Q}(a) \cong \mathbb{Q}(b)$, with $\lambda + \mu a + \gamma a^2 \mapsto \lambda + \mu b + \gamma b^2$.*

Example. *Variant $p(x) = x^2 - 2$, two roots in $\mathbb{C}$ are $+\sqrt{2}$ and $-\sqrt{2}$, therefore $\mathbb{Q}(+\sqrt{2}) \cong \mathbb{Q}(-\sqrt{2})$, $\lambda + \mu\sqrt{2} \mapsto \lambda - \mu\sqrt{2}$, Note $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$, but the isomorphism we just got was* not *the identity.*

Bits missing?

Tower Law

Notation. *If $K \subseteq L$, then define $[L : K] = \dim_K L$, the dimension of L as a K-vector space.*

Basic idea: If $K \subseteq L$ are fields and V is a vector space over L, then V is also a vector space over K.

Notation. *The dimension can change.*
Indeed $\mathbb{R} \subseteq \mathbb{C}$ and $V = \mathbb{C}^n \cong \mathbb{R}^{2n}$. $\dim_{\mathbb{C}} V = n$, $\dim_{\mathbb{R}} V = 2n$, because ($\dim_{\mathbb{R}} \mathbb{C} = 2$)

Example. $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$

Proposition 2.5. *If $K \subseteq L \subseteq M$ are fields, then $[M : K] = [L : K] \times [M : L]$.*

Remark. *If $K \subseteq L$ and V is a vector space over L then $\dim_K V = \dim_L V \times [L : K]$, and the proof is the same.*

Remark. *If any of these quantities are infinite, then interpret the equation as $\infty = \infty$.*
i.e. $[M : K] = \infty \iff [M : L] = \infty$ or $[L : K] = \infty$.
The proof will only consider the result for finite extensions.

Proof. Say $[M : L] = d$ and $[L : K] = e$ and $d, e \in \mathbb{Z}_{\geq 1}$.
Say $m_1, m_2, \ldots, m_d$ is a basis for M considered as a vector space over L.
Say $l_1, l_2, \ldots, l_e$ is a basis for L as a vectors space over K.
Let us define $n_{ij} = m_i l_j \in M$ (for $1 \leq i \leq d$ and $1 \leq j \leq e$), these are hence de elements n_{ij}.

Claim. *The n_{ij} are a basis for M as a K-vector space.*

Span: Say $m \in M$, Then

$$m = \sum_{i=1}^{d} \lambda_i m_i$$

for some $\lambda_i \in L$, simply by the definition of m_i. Furthermore, each $\lambda_i \in L$, therefore for each λ_i we have

$$\lambda_i = \sum_{j=1}^{e} \kappa_{ij} l_j$$

for some $k_{ij} \in K$, by the definition of l_j, so

$$\begin{aligned} m &= \sum_{i=1}^{d} \sum_{j=1}^{e} \kappa_{ij} l_j m_i \\ &= \sum_{ij} \kappa_{ij} n_{ij} \end{aligned}$$

Therefore the n_{ij} span M as a K-vector space.
Linear independence: Say $\alpha_{ij} \in K$ and

$$\begin{aligned} \sum_{i=1}^{d} \sum_{j=1}^{e} \alpha_{ij} n_{ij} &= 0 \\ \sum_{i=1}^{d} \sum_{j=1}^{e} \alpha_{ij} m_i l_j &= 0 \\ \sum_{i=1}^{d} \underbrace{\left(\sum_{j=1}^{e} \alpha_{ij} l_j \right)}_{\text{call this } \lambda_i \in L} m_i &= 0 \end{aligned}$$

But the m_i are a basis for M as a L-vector space and $\lambda_i \in L$, therefore m_i are linearly independent over L, so all $\lambda_i = 0$.
Therefore $\sum_{j=1}^{e} \alpha_{ij} l_j = 0 \ \forall i$, but $\alpha_{ij} \in K$ and the l_j are linearly independent over K, therefore $\alpha_{ij} = 0 \ \forall j \forall i$, therefore n_{ij} are linearly independent. □

Reminder of 2.3, $a \in L$ is algebraic over K iff $[K(a) : K] < \infty$
Set-up: $K \subseteq L$ are fields, we say L is finite over K if $[L : K] < \infty$. We say L is algebraic over K if $\forall \lambda \in L$, λ is algebraic over K

Example. $\mathbb{C}$ *is finite over* $\mathbb{R}$ *as* $[\mathbb{C} : \mathbb{R}] = 2$. $\mathbb{C}$ *is algebraic over* $\mathbb{R}$ *because if* $z = x + iy \in \mathbb{C}$, *then* z *is the root of* $T^2 - 2xT + (x^2 + y^2)$.

Corollary 2.6. *If* L *is a finite extension of* K, *then* L *is an algebraic extension of* K.

Proof. Assume $[L : K]$ is finite. Say $\lambda \in L$. Then $K \subseteq K(\lambda) \subseteq L$, therefore $\dim_K K(\lambda) \leq \dim_K L = [L : K] < \infty$.
So by 2.3(b), λ is algebraic over K. □

Corollary 2.7. $K \subseteq L$, *say* $\alpha, \beta \in L$ *are both algebraic over* K. *Then* $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, α/β *(if* $\beta \neq 0$*), are also algebraic over* K.

Proof. α algebraic over K, so $[K(\alpha) : K] < \infty$, β is algebraic over K, therefore β is algebraic over $K(\alpha)$. So $K(\alpha)(\beta) = K(\alpha, \beta)$ is finite dimensional over $K(\alpha)$ $[K(\alpha, \beta) : K(\alpha)] < \infty$, now by the tower law $[K(\alpha, \beta) : K] < \infty$.
By 2.6 $K(\alpha, \beta)$ is an algebraic extension over K, so $\alpha + \beta$, $\alpha - \beta$, $\alpha\beta$, α/β (if $\beta \neq 0$) are all in $K(\alpha, \beta)$, therefore are all algebraic over K. □

Chapter 3

Ruler and Compass constructions

Recall. *The tower law: $K \subseteq L \subseteq M$, fields. Then $[M : K] = [M : L][K : L]$.*

We can use this to resolve three questions which stymied the ancients:
You have a straight-edge and a pair of compasses. What can you do?
We can make a regular hexagon, bisect a line, bisect an angle.
We cannot trisect an angle, duplicate a cube (construct $\sqrt[3]{2}$) or square the circle (given a circle construct a square with the same area, construct length π, given 1).
Let us prove the latter are impossible to do.
Set-up: $S \subseteq \mathbb{R}^2$, a finite set of points. Idea: We say $t \in \mathbb{R}^2$ is constructible in one step from S, if t is a point of intersection of two curves C_1 and C_2, where C_i is either

1. a line drawn between two distinct points $s_1, s_2 \in S$.

2. a circle, with centre $s \in S$, and radius being the distance between two points $s_1, s_2 \in S$.

We say $u \in \mathbb{R}^2$ is constructible from S, if there is a sequence $t_1, t_2, \ldots, t_n = u$ such that each $t_i \in \mathbb{R}^2$ is constructible in one step from $S \cup \{t_1, \ldots, t_{i-1}\}$.
Now start with $S = \{(0, 0), (1, 0)\}$.
So what is constructible?
We can get $(n, 0), n \in \mathbb{Z}$ and then $(q, 0), \in \mathbb{Q}$.

Remark. *We can only construct countably many points from $\{(0, 0), (0, 1)\}$, because we always have a finite number of options, from a finite number of points, so there are points we cannot construct.*

Definition. *If $S = \{p_1, p_2, \ldots, p_n\}$ with $p_i = (x_i, y_i) \in \mathbb{R}$, then let us define $\mathbb{Q}(S) = \mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_n, y_n) \subseteq \mathbb{R}$.*

Idea, we can say something about $[\mathbb{Q}(S) : \mathbb{Q}]$.

Lemma 3.1. *If $S \subseteq \mathbb{R}^2$ is a finite set of points, if $K = \mathbb{Q}(S)$ and if t is constructible in one step from S, and $t = (x, y)$, then $[K(x) : K] = 1$ or $[K(y) : K] = 2$.*

Proof. t is on C_1 and C_2 (notation as above), therefore t is a solution to two equations.
Cases depending on the nature of the C_i (i.e. are they two lines, a line and a circle or two circles?)

1. Say C_1 is a line through s_1, s_2, with $t = mX + c$, with $m, c \in K$.
   Say C_2 is a circle, with centre (a, b) and radius

   $$r = \sqrt{(a_3 - a_4)^2 + (b_3 - b_4)^2}$$

   which is the distance between (a_3, b_3) and $(a_4, b_4) \in S$. So the equation is

   $$(X - a)^2 + (Y - b)^2 = r^2$$

   So what is $C_1 \cap C_2$? Substitute $Y = mX + c$ into the C_2-equation. So now we get a new quadratic equation $p(X) = 0$, with $p(X) \in K[X]$ a polynomial of degree 2.

   (a) t is the root of $p(X)$, if $p(x)$ is irreducible then $[K(t) : K] = 2$, as $p(x)$ is the minimal polynomial of x over K.

   (b) $p(X)$ is reducible, then $t \in K$, so $K(t) = K$, and $[K(t) : K] = 1$

2. C_1 and C_2 are both lines, then $C_1 \cap C_2$ is a point and the coefficients (x, y) of the point will be in K.

3. Last case C_1 and C_2 are both circles. We need to solve

   $$(X - a)^2 + (Y - b)^2 = c \tag{3.1}$$

   and

   $$(X - d)^2 + (Y - e)^2 = f \tag{3.2}$$

   with $a, b, c, d, e, f \in K$. If we try to solve these two equations, we can solve (3.2)-(3.1) and (3.1), which is a line and a circle. And we have already done that in case 1.

□

Corollary 3.2. *S, t, K as above. Then $[K(x, y) : K] = 1, 2, 4$.*

Proof. $[K(x) : K] = 1, 2$, it equals iff $K(x) = K$ iff $x \in K$.
If $x \in K$, then $K(x, y) = K(y)$, so $[K(x, y) : K] = [K(y) : K] = 1$ or 2.
If $x \notin K$, then $[K(x) : K] = 2$. Cases:

1. $y \in K(x)$, then $K(x, y) = K(x)$, and $[K(x, y) : K] = [K(x) : K] = 2$.

2. $y \notin K(x)$, therefore the minimal polynomial of y over $K(x)$ has degree at least 2. But $y \notin K(x)$, so $y \notin K$, so $[K(y) : K] = 2$. So the minimal polynomial of y over K has degree 2.
   So there exists $p(t) \in K[t]$, irreducible, degree 2, such that $p(y) = 0$. But $K \subseteq K(x)$, so we can think of $p(t)$ as being in $K(x)[t]$, and $p(y) = 0$, so the minimal polynomial of y over $K(x)$ has degree ≤ 2.
   So it has degree 2.
   Therefore $[K(x, y) : K(x)] = [K(x)(y) : K(x)] = 2$,by 2.3.
   And $[K(x) : K] = 2$, so $[K(x, y) : K] = [K(x, y) : K(x)][K(x) : K] = 2 \times 2 = 4$

□

Corollary 3.3. *Say S is a finite set of points. $S = \{p_1, p_2, \ldots, p_m\}$, with $p_i = (x_i, y_i)$ and let $K = \mathbb{Q}(x_1, y_1, x_2, y_2, \ldots, x_m, y_m)$. Say $t = (x, y)$ is constructible from S.*
Then $[K(x, y) : K] = 2^d$, for some $d \in \mathbb{Z}_{\geq 0}$.
Moreover, $[K(x) : K]$ and $[K(y) : K]$ are also powers of 2.

Lemma 3.4. *$K \subseteq L \subseteq M$ fields and $[M : K]$ is a (finite and) a power of 2. Then $[L : K]$ is also a power of 2.*

Proof. $[M : K] = [M : L][L : K]$, by the tower law, the result follows immediately. □

Proof of 3.3. K is a field generated by coordinates of points in S. $t_1, t_2, \ldots, t_N = t$. Say $t_i = (\alpha_i, \beta_i)$. By 3.2, $[K(\alpha_1, \beta_1) : K] = 1, 2, 4$, a power of 2.
By 3.2 applied to $S \cup \{t_1\} \cup \{t_2\}$ $[K(\alpha_1, \beta_1, \alpha_2, \beta_2) : K(\alpha_1, \beta_1)] = 1, 2, 4$, a power of 2, so by the tower law, $[K(\alpha_1, \beta_1, \alpha_2, \beta_2) : K] = (1, 2, 4) \times (1, 2, 4)$, a power of 2. By induction, $[K(\alpha_1, \beta_1, \ldots, \alpha_N, \beta_N) : K]$ is a power of 2.
Set $M = K(\alpha_1, \beta_1, \ldots, \alpha_N, \beta_N)$ and apply the 3.4 to $K(x), (y), K(x, y) \subseteq M$. □

As a consequence, if we start with $S = \{(0, 0), (1, 0)\}$, (so $K = \mathbb{Q}$) and we construct a point $t = (x, y)$ with ruler and compasses, then $[\mathbb{Q}(x) : \mathbb{Q}]$ and $[\mathbb{Q}(y) : \mathbb{Q}]$ must be powers of 2.

Now let us beat the ancient Greeks at their own game

Claim (1)**.** *You can not duplicate the cube. i.e. given $S = \{(0, 0), (1, 0)\}$, can not construct 2 points such that the distance between them is $\sqrt[3]{2}$.*

Proof. If we could, we would be able to construct the points $(\sqrt[3]{2}, 0)$.
But if $x = \sqrt[3]{2}$, then x is a root of $t^3 - 2 = 0$ and $t^3 - 2$ is irreducible (by Eisenstein, or otherwise). So $t^3 - 2$ is the minimal polynomial of x, so $[\mathbb{Q}(x) : \mathbb{Q}] = 3$, which is not a power of 2. □

Claim (2)**.** *You cannot trisect a general angle.*

Proof. From $S = \{(0, 0), (1, 0)\}$, we can easily build an angle of $60°$. Say this angle could be trisected. Then it would be possible to construct the point $(x, y) = (\sin(20°), \cos(20°))$.
Recall $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$. If $x = \cos(20°)$, then $4x^3 - 3x = \cos(60°) = \frac{1}{2}$. Therefore $8x^3 - 6x - 1 = 0$. By earlier work, this is irreducible.
So $[\mathbb{Q}(x) : \mathbb{Q}] = 3$, which is a contradiction. □

Claim (3)**.** *We can not square the circle*

Proof. If $x = \pi$, then $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ by Lindemann, which is not a power of 2. □

Chapter 4

Splitting Fields

Galois theory is the study of "permuting around" the roots of a polynomial.

Example. *$K = \mathbb{R}$, $p(x) = x^2 + 1$. $\mathbb{C}$ is the field you get by throwing in all the roots of $p(x)$. Complex conjugation swaps the roots around.*
Something about future isomorphisms. ($\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong C_2 \cong S_2$*)*

Reminder:

If K is a field and $p(x) \in K[x]$ is an irreducible polynomial, then we have seen two ways of building a bigger field containing a root of $p(x)$.
If $K \subseteq \mathbb{C}$ then life is easy, $\mathbb{C}$ is algebraically closed, so let $z \in \mathbb{C}$ be a root of $p(x)$ and set $L = K(z)$. We saw that $[L : K] = \deg p(x)$.
We also saw the abstract approach. Set $M = K[x]/I$, where I is the ideal generated by $p(x)$. We showed (2.4), that M is a field, $p(x)$ has a root in M, $[M : K] = \deg p$.
We also showed that $M \cong L$, if $K \subseteq \mathbb{C}$.

Remark. *$K = \mathbb{Q}$, $p(x) = x^3 - 2$, say $z_1 = \sqrt[3]{2} \in \mathbb{R} \subseteq \mathbb{C}$ and $z_2 = \omega\sqrt[3]{2}$, $\omega = e^{2\pi i/3}$. Then $\mathbb{Q}(z_1) \neq \mathbb{Q}(z_2)$, but both are isomorphic to $\mathbb{Q}[x]/I$, so $\mathbb{Q}(z_1) \cong \mathbb{Q}(z_2)$.*

Definition. *K a field, $p(x) \in K[x]$ any non-zero polynomial (not necessarily irreducible). We say that a field extension $L \supseteq K$ is a* splitting field *for $p(x)$ over K if*

1. *$p(x) = c\prod_{i=1}^{d}(x - \alpha_i)$, $\alpha_i \in L$, $c \neq 0$, i.e. p factors into linear factors in L.*
2. *$L = K(\alpha_1, \alpha_2, \ldots, \alpha_d)$, in other words, L is generated by the roots of $p(x)$.*

Remark. *We just saw above that $\mathbb{Q}(z_1) \cong \mathbb{Q}(z_2)$ and more generally, if you "throw in one root, what you get is well-defined up to isomorphism".*

We want to show that, if L_1 and L_2 are both splitting field for K, then $L_1 \cong L_2$. Back to this later.

Idle Question:

Say $K = \mathbb{Q}$, $p(x)$ an irreducible polynomial of degree 3. L is the splitting field. What is $[L : K]$?

Example. *Say* $p(x) = x^3 - 2$, $K = \mathbb{Q}$. $z_1 = \sqrt[3]{2}$, $z_2 = \omega z_1$, $z_3 = \omega^2 z_3$. $L = \mathbb{Q}(z_1, z_2, z_3)$.
$M = \mathbb{Q}(z_1)$. *Here,* $p(x) = (x - z_1)q(x)$, *where* $q(x)$ *has degree* 2. *Roots of* $q(x)$ *are* z_2 *and* z_3, *but* $z_2, z_3 \notin \mathbb{Q}(z_1) \subseteq \mathbb{R}$.
So $q(x) \in M[x]$ *has degree* 2 *and no roots, so it is irreducible, so* $[M(z_2) : M] = 2$. *Now* $z_2 \in M(z_2)$, *and* $z_3 = -z_2 - z_1 \in M(z_2)$, *So* $L = M(z_2)$. *By the tower law, the splitting field has degree* 6 *(with respect to* $\mathbb{Q}$.*)*

Example. $\cos(20°)$. *From chapter* 3, $c = \cos(20°)$, $4c^3 - 3c = 1/2$. *Set* $d = 2c$, $d^3 - 3d - 1 = 0$ *is irreducible.*
Set $p(x) = x^3 - 3x - 1$. *What is the splitting field?*
In $M[x]$, $p(x)$ *factors as* $(x - d)q(x)$, *but* q *is reducible in* $M[x]$, *turns out the two roots of* $q(x)$ *are* $-1 - 1/d$ *and* $-1/(1 + d)$.
Indeed we check that these are in M. *So the splitting field has dimension* 3.

Example. p *prime,* $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, *is irreducible by Eisenstein-corollary. The roots of* $f(x)$ *are* $\omega, \omega^2, \ldots, \omega^{p-1}$, $\omega = e^{2\pi i/p}$, *so* $\mathbb{Q}(\omega)$ *is the splitting field, it contains* $\omega^2, \ldots$ *because it is a field, so* $\mathbb{Q}(\omega)$ *is the splitting field.*

Say K is a field, $p(x) \in K[x]$ is non-zero. $K \subseteq L$, $K \subseteq M$.
Say $p(x) = (p - l_1)(p - l_2) \ldots (p - l_d)$, $l_i \in L$ and $L = K(l_1, l_2, \ldots, l_d)$.
Say also $p(x) = (x - m_1)(x - m_2) \ldots (x - m_d)$, $m_i \in M$ and say $M = K(m_1, m_2, \ldots, m_d)$.
Is it clear that $L \cong M$?, Is it even clear that $[L : K] = [M : K]$?

Definition. K *a field,* $p(x) \in K[x]$ *a non zero-polynomial. Say* $K \subseteq L$. *We say* $p(x)$ *splits completely in* L *if* $p(x) = c(x - l_1)(x - l_2) \ldots (x - l_d)$, $l_i \in L$.

Definition. *Now say* K *is a field,* $p(x) \in K[x]$ *a non-zero polynomial, and* $K \subseteq L$, L *another field. We say that* L *has property* $*$ *for the pair* $(K, p(x))$, *whenever* $K \subseteq M$, M *any field, then* $p(x)$ *splits completely in* M *if and only if there is an injective homomorphism of field* $\alpha : L \to M$ *such that* α *restricted to* $K \subseteq L$ *is the identity* $K \to K$.

Remark. *Informally,* $K \hookrightarrow M$, *and* $K \hookrightarrow L \xrightarrow{\alpha} M$, *and we want the two ways of going from* K *to* M *to be the same map.*

Remark. *Say* L *has property* $*$ *for* (K, p). *Set* $M = L$, α *is the identity, then that means that* $p(x)$ *splits completely in* L.

Lemma 4.1. *Given a field* K *and* $p(x) \in K[x]$ *non-zero, there exists a field* $L \supseteq K$ *with property* $*$ *for* $(K, p(x))$ *and furthermore* $[L : K]$ *is finite.*

Proof. We proof the following statement: $Q(n)$ = "for any field K and any $p(x) \in K[x]$ of degree n, there exists $L \supseteq K$ with property $*$ for (K, p) and $[L : K]$ is finite."
We will prove $Q(n)$ by induction on n.
$n = 0$ and $n = 1$ are easy: Set $L = K$. (If $\deg(p(x)) \leq 1$ then all roots of $p(x)$ are in K).

Inductive step: $n \geq 0$, and assume $Q(n-1)$ is true.
$p(x)$ degree $n \geq 2$ in $K[x]$. Choose $q(x)$, an irreducible factor of $p(x)$ in $K[x]$. Set $F = K[t]/I$, where $I = (q(t))$, multiples of $q(t)$. So F is K with one root of $q(x)$ thrown in,call this root a. In $F[x]$, $p(x)$ has a root, namely $x = a$.
So $p(x) = (x-a)r(x)$ in $F[x]$, with $\deg(r(x)) = n-1$. By induction there exists some field $L \supseteq F$, satisfying property $*$ for $(F, r(x))$, with $[L : F]$ finite.

Claim. *L satisfies property $*$ for $(K, p(x))$, and furthermore $[L : K]$ is finite.*

Firstly $[L : K] = [L : F][F : K]$, $[L : F]$ is finite by inductive hypothesis, and $[F : K]$ is the degree of $q(x)$, which is finite.
(By the remark after the definition of property $*$, $r(x)$ splits completely in L, $a \in F \subseteq L$, therefore $p(x)$ spits completely in L.)
Let us check that L satisfies $*$ for $(K, p(x))$, if M is a field and $\alpha : L \hookrightarrow M$ is an injective field homomorphism, which is the identity on K, then $p(x)$ splits completely in M (roots in $L - \{l_1, l_2, \ldots, l_n\}$, so the roots in M are $\alpha(l_1), \ldots, \alpha(l_n)$).
Conversely, if $K \subseteq M$ and p splits complete in M, then ($\deg(p) \geq 0$) M contains a root b of $p(x)$. By 2.4, there exists a map $F \hookrightarrow M$, identity on K, sending a to b. By property $*$, $r(x)$ splits completely in M, so there exists a map $L \overset{\alpha}{\hookrightarrow} M$, identity on F. Therefore $\alpha : L \to M$, is the identity on $K \subseteq F$. □

Lemma 4.2. *K, $p(x)$ as above. Say L_1 and L_2 are two fields satisfying $*$ for (K, p) and $[L_1 : K] < \infty$ and $[L_2 : K] < \infty$, then $L_1 \cong L_2$.*

Proof. L_1 satisfies $*$, therefore $p(x)$ splits completely in L_1. Applying $*$ to L_2 with $M = L_1$, we deduce there si a map of fields $L_2 \to L_1$ which is the identity on K.
Any field-map is injective, so $[L_2 : K] \leq [L_1 : K]$. Similarly $[L_1 : K] \leq [L_2 : K]$, hence $[L_2 : K] = [L_1 : K]$, hence the injection $L_2 \to L_1$ is a K-linear injection, between two vector spaces of same dimension, hence it is a bijection, so it is an isomorphism. □

Proposition 4.3. *K a field, $0 \neq p(x) \in K[x]$. Then the following are equivalent for an extension L of K:*

1. *L satisfies $*$ for (K, p).*
2. *L is a splitting field for p over K.*

Proof.
$1 \implies 2$. Say L satisfies $*$. Then $p(x)$ splits completely in L. Say $p(x) = c(x-\alpha_1)\ldots(x-\alpha_n)$, $\alpha_i \in L$. Set $M \subseteq L$ be the field $K(\alpha_1, \ldots, \alpha_n)$. We want $M = L$.
Note $[M : K] < \infty$ by the tower law. Moreover $p(x)$ splits completely in M. Hence by $*$ there is a field map $L \to M$, with the identity on K. Hence $[L : K] \leq [M : K]$, and $M \subseteq L$, so $[L : K] = [M : K]$, so $L = M$.
$1 \impliedby 2$. Say L is a splitting field for $p(x)$ over K. $p(x) = (x-\alpha_1)\ldots(x-\alpha_n)$, $\alpha_i \in L$ and $L = K(\alpha_1, \ldots, \alpha_n)$. We want to show that L satisfies $*$. By 4.1 there does exist some field $L_1 \supset K$ satisfying $*$ such that $[L_1 : K] < \infty$. Now $p(x)$ splits completely in L, therefore there exists a field map $L_1 \to L$, identity on K.
Let us regard L_1 as a subfield of L via this injection. (We want $L_1 = L$)

Clearly $K \subseteq L_1$. Moreover L_1 satisfies $*$, so $p(x)$ splits completely in L_1, so all the $\alpha_i \in L_1$. Hence $L_1 \supseteq K(\alpha_1, \ldots, \alpha_n) = L$. So $L_1 = L$. □

Remark. *Prof. Buzzard: I apologize for this, but I don't apologize that the course isn't completely content-free.*

Corollary 4.4. *If L_1 and L_2 are splitting fields for $p(x)$ over K then $L_1 \cong L_2$.*

Proof. $[L_1 : K] < \infty$ and $[L_2 : K] < \infty$, so the result follows from 4.3 and 4.2. □

Algebraically closed fields & algebraic closures

Proofs were not covered in lectures. Potential mastery material.

Definition. *A field K is algebraically closed if every $0 \neq p(x) \in K[x]$ has all its roots in K.*

Remark. *Equivalently K is algebraically closed if every non-zero polynomial has at least one root. Equivalently $p(x) \in K[x]$ is irreducible if and only if* $\deg p(x) = 1$.

Example. $K = \mathbb{C}$.

Exercise. *If $M = \{x \in \mathbb{C} : x$ is algebraic over $\mathbb{Q}\}$ then M is algebraically closed. (Remark: M is countable)*

Fundamental Fact

If K is any field then $\exists\ M \supseteq K$ such that M is algebraically closed.

Proof. Transfinite Induction and Zorn's Lemma. Keep adding roots of polynomials until you have added them all. □

In fact, we can then replace M by the subfield $\{x \in M : x$ algebraic over $K\}$ and get "smallest" algebraically closed field containing K.

Notation. *$\overline{K}$ is the "smallest" algebraically closed field containing K, call it the* algebraic closure *of K.*

bits missing! definition of algebraic extensions etc

Definition. *Say $K \subseteq L$ are fields and assume ${}^{L}/_{K}$ is algebraic (${}^{L}/_{K}$ is notation for L over K). We say ${}^{L}/_{K}$ is a normal extension if the following is true: If $p(x) \in K[x]$ is any irreducible polynomial such that $p(x)$ has a root in L then $p(x)$ splits completely in L.*

Remark. *${}^{L}/_{K}$ is normal if $\forall p(x) \in K[x]$ irreducible, then if $p(x)$ has a root in L, p splits completely in L.*

Example. *$K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Then $[L : K] = 3$, so ${}^{L}/_{K}$ is finite, hence algebraic. Try $p(x) = x^3 - 2 \in K[x]$ is irreducible, It has a root in L, but $p(x)$ does not split completely since the other two roots are not in $\mathbb{R}$, let alone L. So L is* not *normal over K.*

Is $\mathbb{Q}(\sqrt{2})$ a normal extension of $\mathbb{Q}$?

It is not so clear how to do it. Is $\mathbb{Q}(\sqrt{2},\sqrt{3})$ a normal extension of $\mathbb{Q}$? This might be hard.

Theorem 4.5. *A finite extension $L \supseteq K$ is normal if and only if $\exists q(x) \neq 0 \in K[x]$ such that L is a splitting field for $q(x)$.*

Proof. $\implies$ $K \subseteq L$, $[L : K] < \infty$ and L is a normal extension of K. Pick a basis $e_1, e_2, \ldots, e_d \in L$ for L as a K-vector space.
L/K is finite and hence algebraic. Let $p_i \in K[x]$ be the minimal polynomial of e_i over K.
L/K is normal, therefore $p_i(x)$ splits completely. Set $p(x) = \prod p_i(x)$. Then $p(x)$ also splits completely in L. Moreover, the subfield generated by K and all the roots of $p(x)$ contains the sub K-vector space of L generated by the e_i, so it is L.
So L is the splitting field of $p(x)$.
$\impliedby$ Say L is a splitting field for some polynomial $f(x) \in K[x]$. Say $p(x) \in K[x]$ is irreducible and sa $\alpha \in L$ is a root of $p(x)$.
Consider $p(x) \in L[x]$. Let is factor it in $L[x]$, $(x-\alpha)$ us a factor. Let $q(x)$ be *any* irreducible factor of $p(x)$ in $L[x]$.
If we prove $\deg q(x) = 1$ we are done. By 2.4 there exists a field $M \supseteq L$ such that M contains a root β of $q(x)$, by shrinking M if necessary, we can assume $M = L(\beta)$ and we know that $[M : L] = \deg(q(x))$.
Note, that f splits completely in L, so f splits completely in M, so $M = L(\beta) \supseteq L$. Moreover, L is the splitting field for f over K, which implies L is the splitting field for f over $K(\alpha)$. Also $M = L(\beta)$ is the splitting field of f over $K(\beta)$.
But $K(\alpha) \cong K(\beta)$. By 4.4 $[L : K(\alpha)] = [L(\beta) : K(\beta)]$ also $[K(\alpha) : K] = [K(\beta) : K]$ by 2.4. By the tower law

$$\begin{aligned}[L : K] &= [l : K(\alpha)][K(\alpha) : K] \\ &= [L(\beta) : K(\beta)][K(\beta) : K] \\ &= [L(\beta) : K]\end{aligned}$$

So $\dim_K L = \dim_K L(\beta) = \dim_K(M) < \infty$. and $L \subseteq M$ so $L = M$. □

Recall. *L/K is a splitting field (for some $0 \neq p(x) \in K[x]$) if and only if L/K is normal.*

Now say $K \subseteq L \subseteq M$ and some of these extensions M/L, M/K, L/K are normal, can we deduce that some of the others are?

Lemma 4.6. *Notation as above. Suppose M/K is normal. Then M/L is normal.*

Remark. *Follows from 4.5 (in the case that $[M : K] < \infty$), however we will do a direct proof as well.*

Proof. Say $p(x) \in L[x]$ is irreducible and $p(x)$ has a root $\alpha \in M$. We want to show that $p(x)$ splits completely in M. Let $q(x)$ be the minimal polynomial of α over K. Then $q(x)$ is irreducible and it has a root $\alpha \in M$.
By normality $q(x)$ splits completely in M. However $q(x) \in K[x] \subseteq L[x]$ and $p(x)$ is irreducible in $L[x]$, therefore $p(x)$ is the minimal polynomial of α over L. So $p(x)$ divides $q(x)$, so $p(x)$ splits completely in M. □

Remark. *Some counter examples to other naive hopes about normality.*

1. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$, *then* ${}^{L}/_{K}$ *is not normal. Set* $M = L(\omega)$, $\omega = e^{2\pi i/3}$, *so* $M = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$. *Then* M *is the splitting field of* $x^3 - 2$ *over* K *and* L, *so* ${}^{M}/_{K}$ *and* M/L *are normal.*

2. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = \mathbb{Q}(\sqrt[4]{2})$. *Then* ${}^{L}/_{K}$ *is normal (*L *is the splitting field of* $x^2 - 2$ *over* K*.) and* ${}^{M}/_{L}$ *is normal (splitting field of* $x^2 - \sqrt{2} \in L[x]$*) but* ${}^{M}/_{K}$ *is not normal, because the irreducible polynomial* $x^4 - 2 \in \mathbb{Q}[x] = K[x]$ *has a root in* M *but cannot split completely because* $M \subset \mathbb{R}$ *and* $x^4 - 2$ *has non-real roots.*

Normal Closure

We will turn this into an example sheet question. Say ${}^{L}/_{K}$ is a finite field extension, not necessarily normal. For simplicity let us just embed L into its algebraic closure $\overline{L}$.
What we want is the smallest subfield of $\overline{L}$ containing L and normal over K.
Here is how to get it: Let $e_1, \dots, e_n$ be a K-basis for L. Let $p_i \in K[x]$ be the minimal polynomial of e_i. And say $p(x) = \prod p_i(x)$, so $p(x) \in K[x]$, therefore $p(x) \in L[x]$ so all the roots of $p(x)$ are in $\overline{L} \supseteq K$. Set $M = K(\alpha_1, \alpha_2, \dots) \subseteq \overline{L}$, where α_i are all the roots of $p(x)$. So M is the splitting field of $p(x)$ over K, so M is normal. Moreover $p(e_i) = 0$, so $e_i \in M \forall i$ and $K \subseteq M$, so $L \subseteq M$. So M is called the normal closure of L over K.

Chapter 5

Separable extensions

Galois Theory is about permuting the roots of polynomials (using field maps like complex conjugation, which permutes the two roots of x^2+1).
We "want enough roots", more precisely can the following happen?
K a field, $p(x) \in K[x]$, irreducible, L the splitting field of $p(x)$ over K. Could $p(x)$ have repeated roots in L?

Set-up in this chapter and basic definitions

K is a field, $f(x) \in K[x]$ an irreducible polynomial. We say $f(x)$ is *separable* over K if all the roots of $f(x)$ in the splitting field are distinct. (By property $*$ this is equivalent to saying that in *any* extension $M \supseteq K$ where f splits completely, f has distinct roots)
A general (possibly reducible) non-zero polynomial $f(x) \in K[x]$ is *separable* if all its irreducible factors are.

Example. *x^2 is separable.*

Example. *$x^3 - 2$ is separable over $\mathbb{Q}$.*

Is every polynomial separable?

Let us try and prove this using calculus. But first some more definitions.

Definition. *Say $K \subseteq L$ are fields and say $\alpha \in L$ is algebraic over K. We say α is separable over K if the minimal polynomial of α over K is separable.*

Definition. *Say $K \subseteq L$ are fields and ${}^{L}/_{K}$ is algebraic (e.g. $[L:K] < \infty$). We say ${}^{L}/_{K}$ is separable if all $\alpha \in L$ are separable.*

Lemma 5.1. *Say $K \subseteq L \subseteq M$ and ${}^{M}/_{K}$ is finite (or more generally algebraic). Say ${}^{M}/_{K}$ is separable, then so are ${}^{L}/_{K}$ and ${}^{M}/_{L}$.*

Proof. ${}^{M}/_{K}$ finite, implies ${}^{L}/_{K}$ and ${}^{M}/_{L}$ are finite (similarly ${}^{M}/_{K}$ algebraic, implies ${}^{L}/_{K}$ and ${}^{M}/_{L}$ are algebraic). Also ${}^{L}/_{K}$ is clearly separable.
Let us now show that ${}^{M}/_{L}$ is separable. Choose $m \in M$, let $q(x) \in L[x]$ be the minimal

polynomial of m over L.
We know ${}^{M}/_{K}$ is separable. So let $p(x) \in K[x]$ be the minimal polynomial of m over K. ${}^{M}/_{K}$ is separable, therefore if $M \subseteq N$, a field in which $p(x)$ splits completely, (eg N is the splitting field for $p(x)$ over M) by separability we know $p(x)$ has distinct roots in N. But $q(x)$ divides $p(x)$, as $p(x) \in L[x]$ and $p(m) = 0$. So $q(x)$ also has distinct roots in N. □

Exercise. *Hard exercise:* ${}^{L}/_{K}$ *and* ${}^{M}/_{L}$ *separable implies* ${}^{M}/_{K}$ *separable. (Currently this is hard since we don't yet know enough)*

Formal Differentiation

Set-up: K: any field, $f(x) \in K[x]$ a polynomial. What is $\mathrm{d}f/\,\mathrm{d}x$? If $K \neq \mathbb{R}$ or $\mathbb{C}$ doing analysis is hard or even impossible. Let us circumvent this by:

Definition. *Differentiation now means:*

$$\begin{aligned} \mathrm{D} : K[x] &\to K[x] \\ \mathrm{D}\left(\sum_{i=0}^{n} a_i x^i\right) &\mapsto \sum_{i=1}^{n} i a_i x^{i-1} \end{aligned}$$

Example. *So* $\mathrm{D}(x^4) = 4x^3$.

Remark. *We have to define what* 4 *is. We just mean* $1+1+1+1$, 1 *is always in our fields. In the definition by* i *we mean the image of* $i \in \mathbb{Z}$.

Lemma 5.2. *If* f *and* $g \in K[x]$ *then* $\mathrm{D}(fg) = f\mathrm{D}(g) + g\mathrm{D}(f)$.

Proof. Step 1: Check it for $f(x) = x^m$ and $g(x) = x^n$.

$$\begin{aligned} LHS &= \mathrm{D}(x^{m+n}) \\ &= (m+n)x^{m+n-1} \\ RHS &= x^n\mathrm{D}(x^m) + x^m\mathrm{D}(x^n) \\ &= mx^{m+n-1} + nx^{m+n-1} \\ &= (m+n)x^{m+n-1} \end{aligned}$$

Step 2: $g(x) = x^n$ and $f(x) \in K[x]$ arbitrary. Think of $g(x)$ as fixed. The maps $K[x] \to K[x]$, $f \mapsto \mathrm{D}(fg)$ and $f \mapsto f\mathrm{D}(g) + g\mathrm{D}(f)$ are both easily checked to be K-linear and they agree if $f(x) = x^m$ by step 1. Therefore they agree on a basis for $K[x]$, hence they agree.
Step 3: Think of $f(x)$ as fixed and consider $g \mapsto \mathrm{D}(fg)$ and $g \mapsto f\mathrm{D}(g) + g\mathrm{D}(f)$. Both are K-linear maps $K[x] \to K[x]$ and they agree on a basis, therefore they agree. □

Lemma 5.3. $\mathrm{D}((x-\alpha)^n) = n(x-\alpha)^{n-1}$

Proof is left as an exercise.

Proposition 5.4. *K a field, $0 \neq f(x) \in K[x]$, $K \subseteq L$ and $f(x)$ splits completely in L. Then the following are equivalent*

1. *$p(x)$ has a repeated root in L.*

2. *There exists $\alpha \in L$ such that $f(\alpha) = 0$ and $(\mathrm{D}f)(\alpha) = 0$.*

3. *$\mathrm{hcf}(f, \mathrm{D}f)$ has positive degree (i.e. is non-constant)*

Proof. 1 $\implies$ 2. 1 $\implies$ $p(x) = (x-\alpha)^n g(x)$, some $g(x) \in L[x]$ and $n \geq 2$, where α is the repeated root. Then

$$\begin{aligned} \mathrm{D}p &= \mathrm{D}((x-\alpha)^n)g(x) + (x-\alpha)^n \mathrm{D}(g(x)) \\ &= n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n \mathrm{D}(g(x)) \end{aligned}$$

$n \geq 2$ implies that this is zero at α.
2 $\implies$ 3. Let $p(x)$ be the minimal polynomial of α, this exists because $f(\alpha) = 0$. Then 2 $\implies$ $p(x) \mid f(x)$ and $p(x) \mid (\mathrm{D}f)(x)$, so $p(x)$ divides the $\mathrm{hcf}(f, \mathrm{D}f)$ and $p(x)$ is non-constant, so the hcf is non-constant.
3 $\implies$ 1. Suppose $h(x)$ has positive degree and h divides both f and $\mathrm{D}f$. Then h splits completely in L. Let $\alpha \in L$ be a root of $h(x)$. Know $f(\alpha) = 0$, so $f(x) = (x-\alpha)g(x)$, so

$$\begin{aligned} \mathrm{D}f &= \mathrm{D}((x-\alpha)g) \\ &= (x-\alpha)\mathrm{D}g + g \end{aligned}$$

so $(\mathrm{D}f)(\alpha) = 0 \implies (\alpha - \alpha)\mathrm{D}(g) + g(\alpha) = 0$, so $g(\alpha) = 0$, so f has a double root at α. □

Corollary 5.5. *Let K be a field and say $f \in K[x]$ is an irreducible polynomial. Say f is* not *separable. Then $Df = 0$.*

Proof. f satisfies 5.4.1, therefore it satisfies 5.4.3, i.e. $h = gcd(f, \mathrm{D}f) > 0$. But h divides f, and f is irreducible. Therefore $\deg h = \deg f$, (and $h = cf$, for some $c \neq 0$).
Also h divides $\mathrm{D}f$. But $\deg(\mathrm{D}f) < \deg f$. So $\mathrm{D}f = 0$. □

Example. *This can happen: $K = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, $f(x) = x^p$. Then $\mathrm{D}f = px^{p-1}$, but $p = 0$ in K so $\mathrm{D}f = 0$. (However f is not irreducible.)*

Remark. *Clearly in general, if $f \neq$ constant and if $\mathrm{D}f = 0$, then K cannot have characteristic 0, as a leading term of f is $a_n x^n$, $a_n \in K$, $a_n \neq 0$, $n \geq 1$, $n \in \mathbb{Z}$.*
So if $\mathrm{D}f = 0$, then $na_n = 0$, so $n = 0$ in K.
So the map $\mathbb{Z} \to K$ has a non-zero Kernel.

Corollary 5.6. *If $f(x) \in K[x]$ is irreducible and separable, then K has characteristic p for some prime number p, and*

$$f(x) = \sum_{i=0}^{m} a_i x^{pi}$$

for some $a_i \in K$.

Proof is left as an exercise.

Definition. *(really bad notation, in Prof Buzzards opinion) A field K is perfect, if every finite extension L of K is separable.*

Remark. *Easy check, this is if and only if every $0 \neq f \in K[x]$ is separable, if and only if every irreducible $f \in K[x]$ is separable.*

Corollary 5.7. *If K as characteristic 0, K is perfect.*

Example. $\mathbb{Q}, \mathbb{R}, \mathbb{Q}(\sqrt{2})$ *are all perfect.*

Proposition 5.8 (Frobenius Map)**.** *Let K be a field, of characteristic $p > 0$. Consider the map* Frob $: K \to K$. Frob$(\lambda) = \lambda^p$. *Then* Frob *is a homomorphism of fields.*

Proof. Need to check Frob$(0) = 0$. Frob$(1) = 1$.
Frob$(\lambda\mu) =$ Frob(λ)Frob(μ). Yes: $(\lambda\mu)^p = \lambda^p\mu^p$
Frob$(\lambda + \mu) =$ Frob$(\lambda) +$ Frob(μ)?
Now

$$(\lambda + \mu)^p = \lambda^p + \binom{p}{1}\lambda^{p-1}\mu + \cdots + \binom{p}{i}\lambda^{p-i}\mu^i + \cdots + \mu^p$$

But p divides $\binom{p}{i}$, for $1 \leq i < p$, so

$$= \lambda^p + \mu^p$$
$$= \text{Frob}(\lambda) + \text{Frob}(\mu)$$

□

Example. $K = {}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$. Frob *is the identity map by Fermat's Little Theorem.*

Example. $K = ({}^{\mathbb{Z}}\!/_{3\mathbb{Z}})(i)$, $i^2 = -1$, *the splitting field of $x^2 + 1$ over* ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$.
$K = \{a + bi : a, b \in {}^{\mathbb{Z}}\!/_{3\mathbb{Z}}\}$, $3 = 0$ *in K, so the characterstic of K is* 3.
Frob$(i) = i^3 = -i = 2i \neq i$. *So* Frob *is not always the identity.*

Lemma 5.9. *If* $\text{char}(K) = p$, *then* Frob *is injective.*

Proof. Frob $: K \to K$ is a group homomorphism. Kernel of Frob is $\{\lambda \in K : \lambda^p = 0\} = \{0\}$ as K is a field. □

Lemma 5.10. *Say K is a field of characteristic $p > 0$ and say $K \to K$ is surjective. Then K is perfect.*

Proof. Say $f \in K[x]$ is irreducible and not separable. Then $\mathrm{D}f = 0$, by 5.5. So

$$f = a_0 + a_i x^p + a_2 x^{2p} + \cdots + a_n x^{np}$$

Frob is surjective, so $a_i = (b_i)^p$ for some $b_i \in K$, so

$$= b_0^p + b_1^p x^p + \cdots + b_n^p x^{np}$$
$$= (b_0 + b_1 x + \cdots + b_x^n)^p$$

This is a contradiction as f is irreducible. □

Corollary 5.11. *If K is a finite field K is perfect.*

Proof. Frob $: K \to K$ is injective by 5.9, therefore surjective as K is finite. □

Example of a non-separable polynomial

Example. *We need a field K such that $p = 0$ in K for some prime number p, but needs to be infinite.*
Idea set K equals to the field of fractions of $(\mathbb{Z}/p\mathbb{Z})[T]$, i.e.

$$K = \left\{ \frac{f(T)}{g(T)} : f, g \in (\mathbb{Z}/p\mathbb{Z})[T], g \neq 0 \right\}$$

$\mathrm{Frob}(f/g) = f^p/g^p$ *the ratio of polynomials in T^p, so* $\mathrm{Frob}(\lambda) = T$ *has no solution.*
Set $p(x) \in K[x]$ to be the polynomial $x^p - T$. Claim: $p(x)$ is irreducible and not separable.

Chapter 6

Galois Extensions and the Fundamental Theorem of Galois Theory

Definition. *An extension $L \supseteq K$ is Galois if it is*

- *algebraic,*
- *normal,*
- *separable.*

Definition. *${}^{L}\!/_{K}$ is finite Galois if it is finite ($[L : K] < \infty$), normal and separable.*

Recall. *An automorphism of an object X is an isomorphism $X \to X$.*

Definition. *$L \supseteq K$, define* $\mathrm{Aut}_K(L) = \{$*isomorphisms* $\phi : L \to L : \phi|_K = \mathrm{id}\}$.

Definition. *If ${}^{L}\!/_{K}$ is Galois, we write* $\mathrm{Gal}({}^{L}\!/_{K}) = \mathrm{Aut}_K(L)$.

Example. *$K = \mathbb{R}$, $L = \mathbb{C}$. L is the splitting field of $x^2 + 1$ over K, so $[L : K] = 2 < \infty$. So ${}^{\mathbb{C}}\!/_{\mathbb{R}}$ is finite and Galois.*
Let us compute $\mathrm{Gal}({}^{\mathbb{C}}\!/_{\mathbb{R}})$.
$\mathrm{Gal}({}^{\mathbb{C}}\!/_{\mathbb{R}})$ *is the field isomorphisms that are the identity on $\mathbb{R}$, so* $\mathrm{id} : \mathbb{C} \to \mathbb{C}$ *is clearly a field isomorphism in* $\mathrm{Gal}({}^{\mathbb{C}}\!/_{\mathbb{R}})$.
Say $\phi : \mathbb{C} \to \mathbb{C}$ is in $\mathrm{Gal}({}^{\mathbb{C}}\!/_{\mathbb{R}})$. *Then $\phi(r) = r$ for all $r \in \mathbb{R}$. What about $\phi(i)$?*
Say $\phi(i) = z \in \mathbb{C}$. ϕ is a field homomorphisms so $\phi(i^2) = \phi(i)^2 = z^2$, but $i^2 = -1$ therefore $\phi(i^2) = \phi(-1) = -1$, so $z^2 = -1$, $z = \pm i$.
Moreover, if we know $\phi(i)$, we know all of ϕ, because a general complex number $\omega = a + bi$, with $a, b \in \mathbb{R}$ so

$$\begin{aligned}\phi(\omega) &= \phi(a + bi) \\ &= \phi(a) + \phi(b)\phi(i) \\ &= a + b\phi(i) \\ &= a + bz\end{aligned}$$

Case 1: $\phi(i) = i$, then $\phi(a+bi) = a+bi$, so ϕ is the identity, which works.
Case 2: $\phi(i) = -i$, then $\phi(a+bi) = a-bi$, so $\phi(\omega) = \bar{\omega}$.
Does this work? Is $\omega \to \overline{\omega}$ an isomorphism? It is a bijection as $\overline{\overline{\omega}} = \omega$.
Furthermore $\overline{0} = 0$, $\overline{1} = 1$ and $\overline{\xi + \omega} = \overline{\xi} + \overline{\omega}$ and $\overline{\xi\omega} = \overline{\xi}\,\overline{\omega}$. Hence complex conjugation is indeed an automorphism of $\mathbb{C}$. So $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \textit{complex conjugation}\}$.

Remark. $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = 2 = [\mathbb{C} : \mathbb{R}]$.

Lemma 6.1. *$\mathrm{Aut}_K(L)$ is a group under composition.*

Proof. The identity map $L \to L$ is the identity of the group.
Associativity is naturally true for composition of functions.
The inverse of an isomorphism is an isomorphism.
Hence $\mathrm{Gal}(L/K)$ is a group if L/K is finite Galois. □

Example. $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong C_2$.

Example. *Let us see what happens when the extension is not normal. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$, not normal, therefore not Galois.*
What is $\mathrm{Aut}_K(L)$? Say $\phi : L \to L$, is an isomorphism and $\phi|_{\mathbb{Q}}$ is the identity. Say $\phi(\sqrt[3]{2}) = z \in L$. As last time $z^3 = \phi(\sqrt[3]{2})^3 = \phi(\sqrt[3]{2}^3) = \phi(2) = 2$.
But $L \subseteq \mathbb{R}$ and the only solution to $z^3 = 1$ in $\mathbb{R}$ is $z = \sqrt[3]{2}$. Therefore $\phi(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$, so $\phi = \mathrm{id}$.
So $\mathrm{Aut}_K(L) = \{\mathrm{id}\}$, a group of size $1 < [L : K] = 3$, but this happens because L/K is not normal.

Example. *A inseparable example.*

$$L = (\mathbb{Z}/p\mathbb{Z})(t) = \left\{ \frac{f(t)}{g(t)} : f, g \in (\mathbb{Z}/p\mathbb{Z})[x], g \neq 0 \right\}$$
$$K \supseteq L = (\mathbb{Z}/p\mathbb{Z})(t^p) = \left\{ \frac{f(t^p)}{g(t^p)} : f, g \in (\mathbb{Z}/p\mathbb{Z})[x], g \neq 0 \right\}$$

$L = K(t)$, and $t^p \in K$, so this is an finite extension, but it is not separable.
If $\phi \in \mathrm{Aut}_K(L)$, then $\phi(t) = z \in L$, satisfying $z^p = \phi(t^p) = t^p$, as $t^p \in K$, so $z^p = t^p$, thus $z^p - t^p = 0$ and furthermore $(z-t)^p = 0$, hence $z = t$, so ϕ is the identity.
Again $|\mathrm{Aut}_K(L)| = 1 < [L : K] = p$, but L/K was not separable.

Example. *$K = \mathbb{Q}$, L the splitting field of $x^3 - 2$. L/K is finite (6) and normal (a splitting field) and separable (characteristic 0).*
What is $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$?
If $\omega = \mathrm{e}^{2\pi i/3}$, $\alpha = \sqrt[3]{2} \in \mathbb{R}$. Then the roots of $x^3 - 2$ are $\alpha, \beta = \alpha\omega, \gamma = \alpha\omega^2$. $L = \mathbb{Q}(\alpha, \beta, \gamma) = \mathbb{Q}(\alpha, \omega)$.
Can we thing of any elements of $\mathrm{Gal}(L/K)$? Identity, Complex conjugation (this will work since $\omega \to \overline{\omega} = \omega^2$).
Say $\phi(l) = \overline{l}$. $\phi(\alpha) = \alpha$, $\phi(\beta) = \gamma$, $\phi(\gamma) = \beta$.
Note, if ψ is any element of $\mathrm{Gal}(L/K)$, then $\psi(\alpha)^3 = \psi(\alpha^3) = \psi(2) = 2$. Therefore $\psi(\alpha) = \alpha$

or β or γ. Similarly for β and γ, and ψ is a bijection. So ψ induces a permutation of $\{\alpha, \beta, \gamma\}$.
$\mathrm{id} \to$ *identity permutation, complex conjugation induces swapping β and γ.*
Is there a field isomorphism $\phi : L \to L$ such that $\psi(\alpha) = \beta$, $\psi(\beta) = \gamma$, $\psi(\gamma) = \alpha$?
Not sure...
Upshot: Injection $\mathrm{Gal}({}^{L}/_{K}) \hookrightarrow S_3$, $|S_3| = 6 = [L : K]$, the permutations of $\{\alpha, \beta, \gamma\}$.

Example. *$f(x) = x^5 - 55x - 88$ and $g(x) = x^5 + 55x - 88$ (irreducible). Now choose one of f and g, so there are five roots $\alpha, \beta, \gamma, \delta, \epsilon$, $L = \mathbb{Q}(\alpha, \beta, \gamma, \delta, \epsilon)$.*
Now does there exist $\psi : L \to L$, field automorphism such that $\psi(\alpha) = \beta$, $\psi(\beta) = \alpha$, $\psi(\gamma) = \gamma$, $\psi(\delta) = \delta$, $\psi(\epsilon) = \epsilon$?
Answer, it does exist for one but not for the other.

Example. *$x^3 - 2$, roots α, β, γ. $L = \mathbb{Q}(\alpha, \beta, \gamma)$, $[L : \mathbb{Q}] = 6$. What are the subfields of L?*
Some of them are $\mathbb{Q}(\alpha), \mathbb{Q}(\beta), \mathbb{Q}(\gamma)$, $\mathbb{Q}(\omega)$, $\omega = \beta/\alpha$.
Are there any more? No! But we do not yet know how to see this using the tools we have.

Fundamental Theorem of Galois Theory

Theorem. *Say ${}^{L}/_{K}$ is a finite Galois extension. Set $G = \mathrm{Gal}({}^{L}/_{K})$ Then*

I. $|G| = [L : K]$

II. There is a natural order-reversing bijection between subgroups of G and fields M with $K \subseteq M \subseteq L$ (subextensions of L). (dictionary: $H \subseteq G \to \{\lambda \in L : h(\lambda) = \lambda \ \forall h \in H\}$)

III. If $H \leftrightarrow M$ is the dictionary of II then ${}^{L}/_{M}$ is finite Galois, and $\mathrm{Gal}({}^{L}/_{M}) = H$ (equals not just isomorphic since ${}^{L}/_{M} \subseteq G$)

IV. H is a normal subgroup of G if and only if M is a normal extension of K and when this happens $\mathrm{Gal}({}^{M}/_{K}) \cong {}^{G}/_{H}$

Say ${}^{L}/_{K}$ is finite. Here is a criterion for normality.

Lemma 6.2. *${}^{L}/_{K}$ is normal if and only if for all field extensions $M \supseteq L$ and for all field maps $\alpha : L \to M$ such that $\alpha|_K$ is the identity, the image of α is L.*

Example. *$K = \mathbb{Q}$, $L = \mathbb{Q}(\alpha)$, $\alpha = \sqrt[3]{2}$, $\beta = \omega\alpha$, $\omega = e^{2\pi i/3}$. Then ${}^{L}/_{K}$ is not normal, $M = \mathbb{C}$, $\psi : \Omega(\alpha) \to \mathbb{C}$, sends α to β. Then ψ is an isomorphism $\mathbb{Q}(\alpha) \to \mathbb{Q}(\beta) \neq \mathbb{Q}(\alpha)$, so $\mathrm{Im}(\psi) \neq L$.*

Proof. Normality $\implies \mathrm{Im}(L) = L$ (exercise sheet 4)
Converse: Say the Image of α is always L and let us prove ${}^{L}/_{K}$ is normal. So let us say $p(x) \in K[x]$ is irreducible and $p(x)$ has a root $\gamma \in L$.
We want to show that $p(x)$ splits completely in L. Set $M = \overline{L}$, the algebraic closure of L. We know ${}^{L}/_{K}$ is finite. Write $L = K(\gamma, \delta_1, \delta_2, \ldots, \delta_r)$. Say $\beta \in \overline{L}$ is a another rots of $p(x)$. Then we know there is a map $K(\gamma) \to \overline{L}$, identity on K sending γ to β.

Since $\overline{L}$ is algebraically closed we can extend this map to a map from $L \to \overline{L}$ (define the image of each δ_i recursively).
This gives us a map $L \to \overline{L}$ identity on K. By hypothesis, image of this map is L. But the image contains β, therefore $\beta \in L$. □

Example. *Say ${}^{L}/_{K}$ is finite. How many field maps $L \to \overline{L}$ are there, which are the identity on K?*
i.e. If $p(x) \in K[x]$ irreducible and $L = K(\alpha)$ with α a roots of $p(x)$ then to give a map $L \to \overline{L}$ as above is to give the image of α, i.e. to give a root of $p(x)$. Therefore the number of maps is the number of roots.

Definition. *Set $[L : K]_S$ the separable degree of L over K is the number of field maps $L \to \overline{L}$, identity on K.*

Lemma 6.3. *If $L = K(\alpha)$ then $[L : K]_S \leq [L : K]$ with equality if and only if α is separable over K.*

Proof. If $p(x)$ is the minimal polynomial of α, then $[L : K]_S$ is the numbr of roots of $p(x)$ by the above discussion. And $[L : K]$ is the degree of $p(x)$ by 2.3. The number of roots in $\overline{L}$ is less or equal than the degree of $p(x)$. With equality if and only if the roots are distinct. Now the roots are distinct if and only if $p(x)$ is separable if and only if α is separable over K. □

Lemma 6.4. *If $K \subseteq L \subseteq M$ all finite then $[M : K]_S = [M : K]_S[L : K]_S$*

Proof. Think of a map $M \to \overline{M}$ as first a map $L \to \overline{M}$ ($[L : K]_S$ choices) followed by an extension of this map to $M \to \overline{M}$ ($[M : L]_S$ choices.) □

Corollary 6.5. *If ${}^{L}/_{K}$ is finite then*

i) $[L : K]_S \leq [L : K]$.

ii) $[L : K]_S = [L : K]$ *if and only if L is a separable extension of K.*

Proof. ${}^{L}/_{K}$ is finite so pick a basis $e_1, \ldots, e_n$. Thus $L = K(e_1, \ldots, e_n)$, now $K \subseteq K(e_1) \subseteq K(e_1, e_2) \subseteq \cdots \subseteq K(e_1, \ldots, e_n)$.

i) By 6.3 $[K(e_1, \ldots, e_{i+1}) : K(e_1, \ldots, e_i)]_S \leq [K(e_1, \ldots, e_{i+1}) : K(e_1, \ldots, e_i)]$ for all i. By 6.4 and tower law the result follows.

ii) $\implies$ Says $\alpha \in L$. We want to show that α is separable over K. Trick $L \supseteq K(\alpha) \supseteq K$. So

$$[L : K] = [L : K(\alpha)][K(\alpha) : K]$$

by the tower law

$$\geq [L : K(\alpha)]_S[K(\alpha) : K]_S$$
$$= [L : K]_S$$

by 6.4.
But $[L:K] = [L:K]_S$, therefore $[K(\alpha):K]_S = [K(\alpha):K]$ and by 6.3, α is separable.
$\Longleftarrow$ Say L/K is separable. Therefore (with notation as above) $K(e_1,\ldots,e_{i+1})/K(e_1,\ldots,e_i)$ is separable (by 5.1). Therefore $[K(e_1,\ldots,e_{i+1}) : K(e_1,\ldots,e_i)]_S = [K(e_1,\ldots e_{i+1}) : K(e_1,\ldots,e_i)]$. By 6.4 and the tower law, deduce $[L:K]_S = [L:K]$.

□

Theorem 6.6. *Say L/K is finite, then $\mathrm{Aut}_K(L)$ is a finite group of size at most $[L:K]$, with equality if and only if L/K is finite Galois.*

Proof.

$$\begin{aligned}\mathrm{Aut}_K(L) &= \{\phi : L \to L : \phi|_K = id\}\\ &\subseteq \{\phi : L \to \overline{L} : \phi|_K = id\}\end{aligned}$$

with equality if and only if L/K is normal by 6.2. But the size of $\{\phi : L \to \overline{L} : \phi|_K = id\}$ is $[L:K]_S \leq [L:K]$ with equality if and only if L/K is separable. □

Remark. *We just proved part I. of the fundamental theorem of Galois Theory.*

The next part of the Fundamental Theorem of Galois Theory relates subfields to subgroups.

Set-up:
L/K finite and Galois. $G = \mathrm{Gal}(L/K)$. Set

$$\begin{aligned}\mathscr{X} &= \{M : \text{ fields } : K \subseteq M \subseteq L\}\\ \mathscr{Y} &= \{H : \text{ subgroups of } G\}\end{aligned}$$

Obviously $\mathscr{Y}$ is a finite set, we know nothing about $\mathscr{X}$.
Fundamental Theorem of Galois Theory says that there exists a bijection $\mathscr{X} \leftrightarrow \mathscr{Y}$. Define

$$\begin{aligned}&\Theta : \mathscr{X} \to \mathscr{Y}\\ &\Theta(M) = \{g \in G : g(m) = m \ \forall m \in M\}\end{aligned}$$

Define

$$\begin{aligned}&\Psi : \mathscr{Y} \to \mathscr{X}\\ &\Psi(H) = \{\lambda \in L : h(\lambda) = \lambda \ \forall h \in H\}\end{aligned}$$

By definition of G, $K \subseteq \Psi(H)$. It is easy to check that $\Psi(H)$ is a field (as $h \in H$ is a field map)
Goal: prove $\Theta \circ \Psi = id_{\mathscr{Y}}$ and $\Psi \circ \Theta = id_{\mathscr{X}}$.

Lemma 6.7.

i) Θ and Ψ are order-reversing.

ii) If $M \in \mathscr{X}$ then $\Psi(\Theta(M)) \supseteq M$ and similarly if $H \sin \mathscr{Y}$, then $\Theta(\psi(H)) \supseteq H$.

iii) $\Theta \circ \Psi \circ \Theta = \Theta$ *and* $\Psi \circ \Theta \circ \Psi = \Psi$.

Proof.

i) is clear from the definitions.
e.g. if $H_1 \subseteq H_2$ then for $\lambda \in L$, $y \in \Psi(H_2)$, then $h(\lambda) = \lambda$ for all $h \in H_2$, therefore $h(\lambda) = \lambda$ for all $H \in H_1 \subseteq H_1$, so $\lambda \in \Psi(H_1)$.
The other argument is the same.

ii) Equally clear.
e.g. if $m \in M$ then for all $h \in \Theta(M)$, $h(m) = m$, therefore $m \in \Psi(\Theta(M))$ by definition.

iii) Follows easily from i) and ii). Apply Θ again and get $\Theta(\Psi(\Theta(M))) \subseteq \Theta(M)$. Conversely, set $H = \Theta(M)$, then ii) implies $\Theta(\Psi(H)) \supseteq H$.

□

Proposition 6.8. $\Psi \circ \Theta = id_{\mathscr{X}}$.

Proof. Say $m \subseteq \mathscr{X}$. Then ${}^{L}/_{M}$ is finite (${}^{L}/_{K}$ finite), normal (4.7) and separable (5.1) therefore ${}^{L}/_{M}$ is Galois. So by 6.6 we know $|\mathrm{Gal}({}^{L}/_{M})| = [L : M]$.
Let $N = \Psi(\Theta(M))$. By 6.7, $M \subseteq N$. We want to show $M = N$.
But by 6.7 iii) $\Theta(M) = \Theta(N)$.
Therefore $\mathrm{Gal}({}^{L}/_{M}) = \mathrm{Gal}({}^{L}/_{N})$ as they are subgroups of $\mathrm{Gal}({}^{L}/_{K})$. Therefore $[L : M] = [L : N]$, but $[L : M] = [L : N][N : M]$ so $[N : M] = 1$, therefore $M = N$. □

Corollary 6.9. Θ *is injective.*

Proof. $\Theta(M_1) = \Theta(M_2) \implies \Psi(\Theta(M_1)) = \Psi(\Theta(M_2)) \implies M_1 = M_2$. □

$\mathscr{Y}$ is finite, $\Theta : \mathscr{X} \to \mathscr{Y}$ injective means $\mathscr{X}$ is finite.

Corollary 6.10. *Say ${}^{L}/_{K}$ is a finite separable extension. Then there are only finitely many intermediate fields $K \subseteq M \subseteq L$.*

Proof. If ${}^{L}/_{K}$ is Galois, then this follows from 6.9.
If ${}^{L}/_{K}$ is not Galois then ${}^{L}/_{K}$ is not normal.
Let N be the normal closure of ${}^{L}/_{K}$, ${}^{M}/_{K}$ is finite, normal and separable. Therefore ${}^{M}/_{K}$ has only finitely many intermediate fields. So ${}^{L}/_{K}$ does too. □

Remark. *Example of a non-separable finite extension with infinitely many intermediate fields is on Example Sheet 5.*

Corollary 6.11 (Theory of the Primitive Element)**.** *Say ${}^{L}/_{K}$ is a finite separable extension. Then there exists $\alpha \in L$ such that $L = K(\alpha)$.*

Remark. *The weird non-separable example earlier is not of this form.*

Proof. Case 1: K is finite (a finite set).
Then L is finite, so $L^\times$ is a finite subgroup of a multiplicative group of a field, so $L^\times$ is cyclic. Then let α be a generator and $L = K(\alpha)$.
Case 2: K is infinite.
Then there are only finitely many M, subfields such that $K \subseteq M \subseteq L$ by 6.10. Define $\mathscr{Z} := \{M : K \subseteq M \subset L\}$.
Each $M \in \mathscr{Z}$ can be considered as a K-vector subspace of the K-vector space L.
Fact from Algebra: If K is an infinite field then a finite dimensional vector space V over K cannot be the union of finitely many proper subspaces.
Hence $L \neq \bigcup_{M \in \mathscr{Z}} M$ so choose $\alpha \in L$, $\alpha \notin M$ for any $M \in \mathscr{Z}$. Then $K(\alpha)$ s an intermediate field that is not in $\mathscr{Z}$, so $K(\alpha) = L$. □

Theorem 6.12. *Let L be a field and let $\mathrm{Aut}(L)$ be the group of field automorphisms. Let $G \subseteq \mathrm{Aut}(L)$ be a finite subgroup. Set $K = \{\lambda \in L : g(\lambda) = \lambda \ \forall g \in G\}$. (Easy check K is a field).*
Then ${}^{L}/_{K}$ is a finite Galois extension, furthermore $\mathrm{Gal}({}^{L}/_{K}) = G$.

Proof. I claim that not only $[L : K] < \infty$ but in fact $[L : K] \leq |G|$. Say $|G| = n$.
Strategy: Take $n + 1$ arbitrary elements $\alpha_1, \ldots, \alpha_{n+1} \in L$. Then show they are K-linearly dependent. Define $V \neq 0$ be the set of maps $G \to L$ (not necessarily group homomorphisms). Then $V \cong L^n$ so is naturally an n-dimensional vector space over L.
If $\phi_1, \phi_2 \in V$ then define $\phi_1 + \phi_2$ by $(\phi_1 + \phi_2)(g) = \phi_1(g) + \phi_2(g)$. If $\lambda \in L$ then define $\lambda\phi_1$ by $\lambda\phi_1(g) = \phi_1(g) \cdot \lambda$.
If $1 \leq i \leq n + 1$, define $\phi_1 \in V$ thus: $\phi_i(g) = g(\alpha_i)$. The ϕ_i give $n + 1$ elements of V, therefore there exists $\lambda_i \in L$ not all zero, such that

$$\sum \lambda_i \phi_i \equiv 0$$

where 0 is the zero-function on G.
With out loss of generality choose the λ_i such that $\lambda_i = 0$ for all $i > r$, where r is as small as possible. We have $\lambda_r \neq 0$. Therefore without loss of generality $\lambda_r = 1$.
We have

$$\sum \lambda_i \phi_i = 0 \tag{+}$$

so for all $g \in G$

$$\sum_{i=1}^{r} \lambda_i \phi_i(g) = 0 \tag{$\times$}$$

Choose $h \in G$ and apply it to $(\times)$

$$\sum h(\lambda_i) h(g(\alpha_i)) = 0 \tag{$\times\times$}$$

$$\therefore \sum h(\lambda_i) \phi_i \equiv 0 \tag{++}$$

Now looking at $(+)-(++)$ implies

$$\sum(\lambda_i - h(\lambda_i))\phi_i \equiv 0$$

But $\lambda_r = 1$, so $h(\lambda_r) = 1$, so $\lambda_r - h(\lambda_r) = 0$, this contradicts the minimality of r unless $\lambda_i = h(\lambda_i)$ for all i and for all h.
So $\lambda_i = h(\lambda_i)$ for all i, h. so $\lambda_i \in K$ for all i.
Substitute $g = \mathrm{id}$ into $(\times)$ so $\sum \lambda_i \alpha_i = 0$,where the λ_i are not all zero.
Say $\alpha \in L$, set $S = \{g(\alpha) : g \in G\}$ (the orbit of α), then $|S| < \infty$ and $|S| \leq |G|$, since $S \subseteq L$.
Define $p(x) = \prod_{s \in S}(x - s) \in L[x]$.
Claim $p(x) \in K[x]$.
For if $g \in G$, then $g : S \to S$ is a bijection, therefore $g(p(x)) = p(x)$, so $p(x) \in K[x]$, indeed, as g was arbitrary.

Claim. *$p(x)$ is the minimal polynomial of α.*

For if $q(x) \in K[x]$ is any polynomial such that $q(\alpha) = 0$, then α is a root of $q(x)$. Now $s \in S$, $s = g(\alpha)$, then $s(\alpha)$ is a root of $g(q(x)) = q(x)$ as the coefficients of q are all in K.
Hence all $s \in S$ are roots of $q(x)$, and therefore $p(x)$ divides $q(x)$. Hence $p(x)$ is the minimal polynomial of α and in particular it is irreducible.
End of the proof of 6.12: ${}^{L}\!/_{K}$ is finite of degree less or equal $|G|$.
Is ${}^{L}\!/_{K}$ normal?
Say $r(x) \in K[x]$ irreducible and monic and $r(x)$ has a root $\alpha \in L$. Let $p(x)$ be as above, then $p(x) = r(x)$ as both are the minimal polynomial of α. Therefore all the roots of $r(x)$ are in L (as they are in S), so ${}^{L}\!/_{K}$ is normal.
Is ${}^{L}\!/_{K}$ separable?
Say $\alpha \in L$. Then (with notation as above) its minimal polynomial of is $p(x)$ which has distinct roots by definition.
But by definition $G \subseteq \mathrm{Gal}({}^{L}\!/_{K})$, therefore $G = \mathrm{Gal}({}^{L}\!/_{K})$, since they have the same size. □

Recall. *The Fundamental Theorem of Galois Theory:*
$L \supseteq K$ finite and Galois, $G = \mathrm{Gal}({}^{L}\!/_{K})$, then

I. $|G| = [L : K]$.

II. Θ *and* Ψ *are order-reversing bijections* $\{$*subgroups of* $G\} \leftrightarrow \{$*intermediate fields* M*, with*$K \subseteq M \subseteq L\}$.

III. If $H \subseteq G$ corresponds to M via this bijection then ${}^{L}\!/_{M}$ is Galois and $\mathrm{Gal}({}^{L}\!/_{M}) = H$.

IV. H is normal in $G \iff {}^{M}\!/_{K}$ is normal, and in this case $\mathrm{Gal}({}^{M}\!/_{K}) \cong G/H$.

Proof of the Fundamental Theorem of Galois Theory.

I. is a consequence of 6.6.

II. $\Psi \circ \Theta$ is the identity by 6.8. and Θ and Ψ are order reversing by 6.7.
So we still have to show that $\Theta \circ \Psi$ is the identity too. In other words, we need to check that if $H \subseteq G$ and $M = \Psi(H) = \{\lambda \in L : h(\lambda) = \lambda \ \forall h \in H\}$, then $\Theta(M) = \{g \in G : g(m) = m \ \forall m \in M\}$ is again H.
But $\Theta(M)$ is the automorphisms of L that fix K and M, which is the automorphisms of L that fix M, $\mathrm{Aut}_M(L)$.
Is ${}^{L}\!/_{M}$ Galois? Yes, by 6.12.(G and K replaced by H and M respectively)
Therefore $\Theta(M) = \mathrm{Gal}({}^{L}\!/_{M}) = H$ by definition of M and 6.12.

III. If $H \leftrightarrow M$, then by definition $M = \{\lambda \in LLh(\lambda) = \lambda \ \forall h \in H\}$, therefore $\mathrm{Gal}({}^{L}\!/_{M}) = H$ by 6.12.

IV. First say ${}^{M}\!/_{K}$ is normal. ${}^{M}\!/_{K}$ is separable by 5.1. and finite therefore ${}^{M}\!/_{K}$ is Galois. Set $Q = \mathrm{Gal}({}^{M}\!/_{K})$.
Now say $g : L \to L$, what is the restriction of g to M? $g|_M : M \to L$, identity on K. By 6.2. (?) the $g(M) = M$ again. Therefore g induces a map $M \to M$, a field isomorphism, identity on K, i.e. an element $\phi(g) \in Q$. So $\phi : G \to Q$.
ϕ is easily checked to be a group homomorphism. SO $\mathrm{Ker}(\phi) \triangleleft G$ is a normal subgroup.
But $\mathrm{Ker}(\phi) = \{g \in G : g(m) = m \ \forall m \in M\} = \Theta(M) = H$.
Therefore H is normal, moreover, by the first isomorphism theorem $G/H \cong \mathrm{Im}(\phi) \subseteq Q$.
But $|G| = [L : K]$, $|H| = [L : K]$ therefore $|G/H| = [M : K] = |Q|$.
So $G/H \cong H$.
Conversely say $H \subseteq G$ is normal. Set $M = \Psi(H) = \{\lambda \in L : h(\lambda) = \lambda \ \forall h \in H\}$. Easy check: if $g \in G$ then $\Psi(gHg^{-1}) = gM$. (Because $\forall m \in M$, $hm = m$, so $(ghg^{-1})(gm) = ghm = gm$)
In our case, H is normal, therefore $gHg^{-1} = H$ for all $g \in G$ and $g(M) = M \forall g \in G$.
So we get a natural map $\mathrm{Gal}({}^{L}\!/_{K}) \to \mathrm{Aut}_K(M)$, $g \mapsto g|_M : M \to M$. Hence we get a group homomorphism $G \to \mathrm{Aut}_K(M)$, and the Kernel is $\Theta(M) = H$.
So we get an injection $G/H \hookrightarrow \mathrm{Aut}_K(M)$. But $|G/H| = [L : K]/[L : M] = [M : K]$, therefore by 6.6. ${}^{M}\!/_{K}$ is Galois and $\mathrm{Gal}({}^{M}\!/_{K}) = \mathrm{Aut}_K(M) = G/H$.

□

Chapter 7

Insolvability of the Quintic

Look at the group theory hand-out on the homepage.
The formula for roots of the quadratic is well known. Similar formulas exist for the cubic and quadratic, only using $+$, $-$, $\times$, $/$, $\sqrt[n]{\ }$.

Theorem 7.1 (Ruffini, Abel 1823)**.** *No such formula exists for the quintic.*

Remark. *Galois gave a far more conceptual proof in the 1840s, which we will see now.*

Strategy:
If there was a formula for the quintic, then the five complex roots of $x^5 - 6x + 3$ would have the form

$$\sqrt[3]{29} + \sqrt[4]{1 + \sqrt{2} \cdot (1 + \sqrt[7]{91})}$$

or something like that.

Definition. *K: a field of characteristic 0. We say a finite extension $L \supseteq K$ is an extension by radicals if there exist fields*

$$K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n = L$$

such that $\forall 0 \leq i < N$, $L_{i+1} = L_i(\alpha_i)$, where $\alpha_i \in L_{i+1}$ and there exists $n_i \in \mathbb{Z}_{\geq 1}$ such that $(\alpha_i)_i^n \in L_i$.

Example. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[7]{91}) \subseteq \mathbb{Q}(\sqrt[7]{91}, \sqrt{2}) \subseteq \mathbb{Q}(\sqrt[7]{91}, \sqrt{2}, \sqrt[4]{1 + \sqrt{2}(1 + \sqrt[7]{91})}) = L$. *Then ${}^{L}\!/_{\mathbb{Q}}$ is an extension by radicals and $L \ni \ldots$.*

Our goal is proving that if $\alpha, \beta, \gamma, \delta, \epsilon$ are the five complex roots of $x^5 - 6x + 3$, then the splitting field $\mathbb{Q}(\alpha, \beta, \gamma, \delta, \epsilon)$ is not contained in L, which is an extension of $\mathbb{Q}$ by radicals.
We have to do two things:

1. Compute $\mathrm{Gal}({}^{M}\!/_{\mathbb{Q}})$, with M the splitting field of $x^5 - 6x + 3$.
2. Find a property of groups such that if ${}^{L}\!/_{K}$, an extension by radicals, then $\mathrm{Gal}({}^{L}\!/_{K})$ has the property, but the group in 1. does not.

Let us do 1. first. $\alpha, \beta, \gamma, \delta, \epsilon$ are the five roots of $x^5 - 6x + 3$. Say M is its splitting field over $\mathbb{Q}$. By Eisenstein, $x^5 - 6x + 3$ is irreducible. Let us say that $[M : \mathbb{Q}] = D$. ${}^{M}\!/_{\mathbb{Q}}$ is finite and normal, it is characteristic 0, so it is separable too, therefore ${}^{M}\!/_{\mathbb{Q}}$ is Galois.
Furthermore $M = \mathbb{Q}(\alpha, \beta, \gamma, \delta, \epsilon)$, therefore if $g : M \to M$ is an element of $\mathrm{Gal}({}^{M}\!/_{\mathbb{Q}})$, then we know that $g(\alpha)$ is a root of $g(x^5 - 6x + 3) = x^5 - 6x + 3$, so $g(\alpha) \in \{\alpha, \beta, \gamma, \delta, \epsilon\}$.
More generally g induces a permutation of $\{\alpha, \beta, \gamma, \delta, \epsilon\}$ and g is determined by this permutation.
Upshot: $\mathrm{Gal}({}^{M}\!/_{\mathbb{Q}}) \subseteq S_5$.
By the tower law: $[M : \mathbb{Q}] = [M : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$, therefore $5 \mid [M : \mathbb{Q}]$, so if $G = \mathrm{Gal}({}^{M}\!/_{\mathbb{Q}})$, $5 \mid |G|$, by the Fundamental Theorem of Galois Theory.
What are the roots of $x^5 - 6x + 3$? Set $f(x) = x^5 - 6x + 3$. Then $f(-1000) < 0$, $f(-1) = 8$, $f(1) = -2$, $f(1000) > 0$. So there are at least three roots (with five being the other possibility).
Now $f'(x) = 5x^4 - 6$, which has two real zeros, therefore f does not have 4 turning points, so f has three roots. So complex conjugation is in $\mathrm{Gal}({}^{M}\!/_{\mathbb{Q}})$ is a transposition, so it swaps 2 of $\{\alpha, \beta, \gamma, \delta, \epsilon\}$.
So far $G \subseteq S_5$, $|G|$ is multiple of 5, so $G \ni$ a transposition.
Fact: This implies $G = S_5$. Proof: See proposition of group theory hand-out.

Part 2. Say ${}^{K}\!/_{L}$ is Galois and an extension by radicals. Then $\mathrm{Gal}({}^{L}\!/_{K})$ is a solvable group.
Fact: A_5 is not a solvable group. Proof: Proposition of hand-out.
Hence if you believe this, roots of $x^5 - 6x + 3$ are not in a radical extension of $\mathbb{Q}$.

Definition. *A finite group G is solvable if $\exists \{1\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_N = G$ where*

1. *$G_1 \triangleleft G_{i+1}$ for all i.*
2. *Quotient groups G_{i+1}/G_i are all abelian.*

Extensions by radicals give us a bunch of subfields, which gives a bunch of subgroups of G (by FTG).
What is left:

Lemma. *Say $K \subseteq L$, and $L = K(\alpha)$ and $\alpha \in L$, and $\beta = \alpha^p = K$, p prime. Say K contains all the pthe roots of unity.*
Then ${}^{L}\!/_{K}$ is Galois and $\mathrm{Gal}({}^{L}\!/_{K})$ is abelian.

Proof. $g(x) = x^p - \beta$.
Simple case $\alpha \in K$, then $L = K$ and we are finished.
Other case, then $\alpha \notin K$, Then $g(\alpha)$ is irreducible, because if g factored then loot a the constant $\alpha^m \in K$ for some $1 \leq m < p$ and $\alpha^p \in K$, therefore $\alpha^{\lambda m + \mu p} \in K$, but there exists λ, μ such that $\lambda m + \mu p = 1$.
So g is irreducible, so L is the splitting field of g. and therefore $[L : K] = \deg(g) = p$, so $|\mathrm{Gal}({}^{L}\!/_{K})| = p$. Therefore $\mathrm{Gal}({}^{L}\!/_{K}) \cong C_p$, which is abelian. □