A twelve hours course in Galois theory

Ken Lee

Autumn 2024

Contents

1 The Galois correspondence **1**

2 Finite extensions and the embedding theorem **5**

3 Normal and separable extensions **9**

4 Galois extensions and the correspondence **12**

5 Cyclotomic extensions, Cyclic extensions **16**

6 Radical extensions **18**

7 Finite fields, Frobenius lifts and existence of non-solvable quintic **21**

8 Bonus : Sneak peak at p-adic and perfectoid fields **26**

1 The Galois correspondence

We show an example of the Galois correspondence. Consider the polynomial $f(T) = T^3 - 2 \in \mathbb{Q}[T]$. Let $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{C}$ be the roots of f.

Slogan : Galois theory studies the "symmetries" of roots of polynomials

To make this precise, let us first investigate the field obtained by chucking in $\alpha_0, \alpha_1, \alpha_2$ to $\mathbb{Q}$. Define

$$\mathbb{Q}_f := \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) := \text{ smallest field in } \mathbb{C} \text{ containing } \mathbb{Q}, \alpha_0, \alpha_1, \alpha_2$$

Question 0 : What does $\mathbb{Q}_f$ look like? We try to describe $\mathbb{Q}(\alpha_0)$ first. Consider the map $T \mapsto \alpha_0$

$$\begin{tikzcd}
\mathbb{Q}[T] \arrow[r, "T\mapsto\alpha_0"] \arrow[d, dashed] & \mathbb{C} \\
\mathbb{Q}(\alpha_0) \arrow[ur, "\subseteq"'] &
\end{tikzcd}$$

The image is $\mathbb{Q}[\alpha_0]$ the collection of polynomial expressions in α_0 with coefficients in $\mathbb{Q}$. Since $f \in \mathbb{Q}[T]$ is irreducible[1] we have $\mathbb{Q}[\alpha_0] = \mathbb{Q}[T]/(f)$ and hence this has a $\mathbb{Q}$-basis $1, \alpha_0, \alpha_0^2$.

- *Exercise 1 : show that for a field K and an K-algebra A which is finite dimensional as a K-vector space and an integral domain, A must be field.*

It follows that $\mathbb{Q}[\alpha_0]$ is a field and hence

$$\mathbb{Q}[\alpha_0] = \mathbb{Q}(\alpha_0)$$

Now we do a trick by observing that

$$\left(\frac{\alpha_1}{\alpha_0}\right)^3 = 2/2 = 1$$

Later on, we will give a way of checking when a polynomial has repeated roots so assume for now that all $\alpha_0, \alpha_1, \alpha_2$ are distinct. Then we get $\alpha_1 = \alpha_0\omega$ for some $\omega \neq 1 = \omega^3$, and similarly $\alpha_2 = \alpha_0\omega^2$. The ω, ω^2 here are called a *primitive cube roots of unity*. They are both roots of the polynomial $T^2 + T + 1 \in \mathbb{Q}[T]$. In the next section, we will be able to show that $\omega \notin \mathbb{Q}(\alpha_0)$. Taking this for granted for now, $T^2 + T + 1$ does not have a root in $\mathbb{Q}(\alpha_0)$, so it is irreducible in $\mathbb{Q}(\alpha_0)[T]$. It follows that

$$\mathbb{Q}[\alpha_0, \omega] \simeq \mathbb{Q}[\alpha_0][T]/(T^2 + T + 1)$$

As a $\mathbb{Q}[\alpha_0]$-vector space, this has dimension two and hence is again a field by Exercise 1. We deduce **Answer 0 :**

$$\mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) = \mathbb{Q}[\alpha_0, \omega] = \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]$$

We now define *the Galois group of f* as

$$G_f := \mathrm{Aut}_{\mathbb{Q}}\, \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) := \{\sigma : \mathbb{Q}_f \to \mathbb{Q}_f \text{ s.t. } \sigma \text{ ring morphism and } \forall\, \lambda \in \mathbb{Q}\,,\, \sigma(\lambda) = \lambda\}$$

Question 1 : Why is this the "symmetries" of $\alpha_0, \alpha_1, \alpha_2$? Observation : any $\sigma \in G_f$ must permute $\{\alpha_0, \alpha_1, \alpha_2\}$. This is ***the* trick** that underlies Galois theory :

$$f(\sigma(\alpha_i)) = (\sigma(\alpha_i))^3 - 2 = \sigma(\alpha_i^3 - 2) = 0$$

Hence we have a well-define group morphism

$$G_f \to \mathrm{Aut}\,\{\alpha_0, \alpha_1, \alpha_2\}$$

Since $\mathbb{Q}_f = \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]$ any $\sigma \in G_f$ is determined by what it does on α_i hence the above morphism is injective. **Answer 1 : The above morphism defines an isomorphism**

$$G_f \simeq \{\sigma \in \mathrm{Aut}\,\{\alpha_0, \alpha_1, \alpha_2\} \text{ s.t. } \forall g \in \mathbb{Q}[X_0, X_1, X_2]\,, g(\alpha_0, \alpha_1, \alpha_2) = 0 \Rightarrow g(\sigma(\alpha_0), \sigma(\alpha_1), \sigma(\alpha_2)) = 0\}$$

in other words, G_f is the permutations of roots of f which preserves all algebraic relations over $\mathbb{Q}$.

Proof. $\mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]$ is precisely the image of the evaluation map

$$\mathbb{Q}[X_0, X_1, X_2] \to \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]\,,\; X_i \mapsto \alpha_i$$

---

[1] Can be checked by Eisenstein's criterion. Alternatively, a cubic over $\mathbb{Q}$ is reducible iff it has a root in $\mathbb{Q}$. This can be checked to be impossible by brute force.

It follows that $\mathbb{Q}[\alpha_0, \alpha_1, \alpha_2] \simeq \mathbb{Q}[X_0, X_1, X_2]/I$ where I is the set of polynomials $g(X_0, X_1, X_2)$ with $g(\alpha_0, \alpha_1, \alpha_2)$. From this, it is clear that G_f lands inside the RHS. Now given $\tilde{\sigma}$ in RHS, one can evaluate

$$\mathbb{Q}[X_0, X_1, X_2] \to \mathbb{Q}[\alpha_0, \alpha_1, \alpha_2]\ ,\ X_i \mapsto \tilde{\sigma}(\alpha_i)$$

Then by definition I is in the kernel of this evaluation map so it factors through the quotient by I to give an automorphism of $\mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ preserving $\mathbb{Q}$. □

Let us now compute G_f. We have the following

$$\mathbb{Q}_f = \mathbb{Q}[\alpha_0, \omega] = \mathbb{Q}[\alpha_0][\omega] \simeq \frac{\mathbb{Q}[\alpha_0][Y]}{(Y^2 + Y + 1)} \simeq \frac{\mathbb{Q}[X][Y]/(X^3 - 2)}{(X^3 - 2, Y^2 + Y + 1)/(X^3 - 2)} \simeq \frac{\mathbb{Q}[X, Y]}{(X^3 - 2, Y^2 + Y + 1)}$$

where the last isomorphism is the 3rd isomorphism theorem of rings. Consider the 3-cycle $\sigma := (\alpha_0\ \alpha_1\ \alpha_2)$. Knowing $\omega = \alpha_1/\alpha_0$ we send $X \mapsto \alpha_1, Y \mapsto \omega$.

$$\begin{tikzcd}
\mathbb{Q}[X,Y] \arrow[r, "\substack{X \mapsto \alpha_1 \\ Y \mapsto \omega}"] \arrow[d, "\substack{X \mapsto \alpha_0 \\ Y \mapsto \omega}"'] & \mathbb{Q}[\alpha_0, \omega] \\
\mathbb{Q}[\alpha_0, \omega] \arrow[ur, dashed, "\simeq"'] &
\end{tikzcd}$$

We get the factoring because $\alpha_1^3 - 2 = 0 = \omega^2 + \omega + 1$ and so $\sigma \in G_f$. Now consider $\tau := (\alpha_0\ \alpha_1)$. Again, since $\omega = \alpha_1/\alpha_0$ we know τ should send $\omega \mapsto 1/\omega = \omega^2$ so we send $X \mapsto \alpha_0, Y \mapsto \omega^2$.

$$\begin{tikzcd}
\mathbb{Q}[X,Y] \arrow[r, "\substack{X \mapsto \alpha_1 \\ Y \mapsto \omega^2}"] \arrow[d, "\substack{X \mapsto \alpha_0 \\ Y \mapsto \omega}"'] & \mathbb{Q}[\alpha_0, \omega] \\
\mathbb{Q}[\alpha_0, \omega] \arrow[ur, dashed, "\simeq"'] &
\end{tikzcd}$$

Again $\alpha_1^3 - 2 = 0 = (\omega^2)^2 + \omega^2 + 1$ gives the above factoring and hence $\tau \in G_f$. It follows that G_f is the whole of $\mathrm{Aut}\,\{\alpha_0, \alpha_1, \alpha_2\}$.

Symmetry means "changes that cannot be observed". The symmetries of a triangle are the ways you can change the triangle such that you cannot tell the difference between before and after. In the same way, G_f are the ways you can swap of roots of f such that as far as $\mathbb{Q}$ can tell, nothing has changed. In this example, there is nothing special about α_0; the whole argument works starting with α_1 or α_2. The roots are equally ambiguous, which is reflected in the quantitative fact that $G_f \simeq S_3$. An example of less ambiguity is $T^3 - 1$. The roots are $1, \omega, \omega^2$. The Galois group of $T^3 - 1$ is cyclic order two generated by $\omega \mapsto \omega^2$. This reflects the fact that 1 is more special than ω, ω^2 whilst the latter cannot be distinguished from each other. Indeed if one writes $\mu := \omega^2$ then $\omega = \mu^2$.

Back to $T^3 - 2$. Observe that $\mathbb{Q} \subseteq \mathbb{Q}_f^{G_f} :=$ the set of elements in $\mathbb{Q}_f$ fixed by G_f. **Claim :** $\mathbb{Q} = \mathbb{Q}_f^{G_f}$**.** Let $x \in \mathbb{Q}_f$ be fixed by G_f. We approach $\mathbb{Q}_f$ this time by adding ω first then α_0. Since $\mathbb{Q}_f = \mathbb{Q}[\omega][\alpha_0]$ we can write

$$x = \lambda_0 + \lambda_1\alpha_0 + \lambda_2\alpha_0^2$$

for $\lambda_i \in \mathbb{Q}(\omega)$. Then since $\sigma(\omega) = \omega$ we have

$$x = \sigma(x) = \lambda_0 + \lambda_1\omega\alpha_0 + \lambda_2\omega^2\alpha_0^2$$

Since $1, \alpha_0, \alpha_0^2$ are a $\mathbb{Q}(\omega)$-basis for $\mathbb{Q}_f$, we can compare coefficients to get $\lambda_1 = \lambda_1\omega$ and $\lambda_2 = \lambda_2\omega^2$ This implies $\lambda_1 = 0 = \lambda_2$ and so $x \in \mathbb{Q}(\omega)$. Now $x = \mu_0 + \mu_1\omega$ for $\mu_i \in \mathbb{Q}$. Then

$$x = \tau(x) = \mu_0 + \mu_1\omega^2 = (\mu_0 - \mu_1) - \mu_1\omega$$

which implies $\mu_1 = -\mu_1$ and so $\mu_1 = 0$. We find that $x \in \mathbb{Q}$. More generally, given any subgroup H of G_f we can compute the *fixed subfield* $\mathbb{Q}_f^H$. Here is a diagram of all the subgroups of G_f and their corresponding fixed subfields.

$$\begin{tikzcd}
& \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2) & & \\
\mathbb{Q}(\omega) \arrow[ur] & \mathbb{Q}(\alpha_0) \arrow[u] & \mathbb{Q}(\alpha_1) \arrow[ul] & \mathbb{Q}(\alpha_2) \arrow[ull] \\
& \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] \arrow[urr] & &
\end{tikzcd}
\qquad
\begin{tikzcd}
& 1 \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
\langle(\alpha_0\ \alpha_1\ \alpha_2)\rangle \arrow[dr] & \langle(\alpha_1\ \alpha_2)\rangle \arrow[d] & \langle(\alpha_0\ \alpha_2)\rangle \arrow[dl] & \langle(\alpha_0\ \alpha_1)\rangle \arrow[dll] \\
& G_f & &
\end{tikzcd}$$

The fundamental theorem of Galois theory says this is all of them. To be more precise, we make some definitions.

> **Definition – Galois extension**
> Let $K \to L$ be an extension of fields. We often identify K with its image in L. We call it *Galois* when there is a finite group $G \subseteq \mathrm{Aut}_K L$ such that $K = L^G$.

The extension earlier $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ was an example of a Galois extension.

> **Proposition – The Galois correspondence**
> Let $K \to L$ be a Galois extension of fields and let $G := \mathrm{Aut}_K L$. Consider the following two constructions :
>
> - Given a subgroup $H \subseteq G$, define L^H as the set of fixed points of L by H. This defines a field containing the image of K.
> - Given a subfield $M \subseteq L$ containing K, define $\mathrm{Aut}_M L$ as the subgroup of G acting trivially on M.
>
> Then we have an order reversing bijection
>
> $$\{\text{subextensions } M \subseteq L\} \underset{\xleftarrow[L^{-}]{}}{\overset{\xrightarrow{\mathrm{Aut\_}L}}{\simeq}} \{\text{subgroups of } \mathrm{Aut}_K L\}$$

The Galois extension $\mathbb{Q}_f/\mathbb{Q}$ is an example of a *solvable* extension.

> **Definition**
> Let $K \to L$ be an extension. We say it is *radical* when there exists a chain of subextensions
>
> $$K = L_0 \to L_1 \to \cdots \to L_{n-1} \to L_n = L$$
>
> such that each $L_{i+1} = L_i(\alpha_i)$ for some α_i with $\alpha_i^{d_i} \in L_i$ for some $d_i > 0$.
>
> For $f \in K[T]$ we say f is *solvable by radicals* when there exists a radical extension $K \to L$ which splits f.

Notice that in the example, that the sequence of groups

$$1 \to \langle(\alpha_0\ \alpha_1\ \alpha_2)\rangle \to G_f$$

is such that one subgroup is normal in the next and furthermore that the factor groups are cyclic. This is an example of a *solvable group*.

> **Definition**
> Let G be a finite group. Then G is called solvable when there exists a chain
>
> $$1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_{n-1} \triangleleft H_n = G$$
>
> such that H_{n+1}/H_n is cyclic.

We will show the following by the end of the course.

> **Proposition – Characteristization of solvable polynomials**
> Let K be a field of characteristic zero and $f \in K[T]$. Then f is solvable by radicals iff G_f is solvable.

> **Proposition**
> The polynomial $T^5 - T - 1 \in \mathbb{Q}[T]$ has Galois group S_5 and hence is not solvable by radicals.

2 Finite extensions and the embedding theorem

We saw in the previous section that $\omega \in \mathbb{Q}(\alpha_0)$ precisely when there is a solution to $T^2 + T + 1$ inside $\mathbb{Q}(\alpha_0)$. Accordingly, there is no copy of $\mathbb{Q}(\omega)$ inside $\mathbb{Q}(\alpha_0)$. This section investigates this phenomenon. We didn't formally define field extensions last time.

> **Definition**
> A field extension is a ring morphism $\iota : K \to L$ between fields.
>
> Since fields have no non-trivial ideals, any field extension $\iota : K \to L$ must be injective. When it is clear, we often identify K with its image ιK. Sometimes we write L/K to say L is an extension of K.

> *Example.*
> *Here is an example of a field extension from a field to itself. Let* $\mathbb{Q}(T) := \operatorname{Frac} \mathbb{Q}[T]$*. Define* $\mathbb{Q}[T] \to \mathbb{Q}[T], T \mapsto T^2$*. Then this induces a field extension* $\mathbb{Q}(T) \to \mathbb{Q}(T)$ *where the image of the first copy is* $\mathbb{Q}(T^2)$*.*

A basic invariant of a field extension is its degree.

> **Definition – Degree of an extension**
>
> Let $K \to L$ be a field extension. Define its *degree* as $[L : K] := \dim_K L$. It is called finite when $[L : K] < \infty$.

When proving things about a finite extension $K \to L$, we will often do so by inducting on $[L : K]$. The following is useful.

> **Proposition – Tower law**
>
> Let $K \to L \to N$ be extensions of fields. Then $[N : K] = [N : L][L : K]$. In particular, a sequence of finite extensions is finite.

The following argument works for infinite extensions, though we will mostly be interested in finite extensions.

Proof. Let $B_L \subseteq L$ be a ι_L-basis and $B_N \subseteq N$ a ι_N-basis. The claim is that $B_L B_N := \{ab \mid a \in B_L, b \in B_N\}$ is a $(\iota_N \circ \iota_L)$-basis of N and has cardinality $B_L \times B_N$.

(Cardinality) Let $(a_1, b_1), (a_2, b_2) \in B_L \times B_N$ such that $a_1 b_1 = a_2 b_2$. This is then a non-trivial L-linear combination of elements in B_N, contradicting linear independence of B_N. The cardinality is thus as desired.

(Linear Independence) Let $\sum_{(a,b) \in B_L \times B_N} \lambda_{a,b} ab = 0$ where $\lambda_{a,b} \in K$ and only finitely many are non-zero. Then we have $\sum_{b \in B_N} \left(\sum_{a \in B_L} \lambda_{a,b} a \right) b = 0$, giving $\sum_{a \in B_L} \lambda_{a,b} a = 0$ by linear independence of B_N, which in turn gives $\lambda_{a,b} = 0$ by linear independence of B_L.

(Spanning) Let $x \in N$. Since B_N is spanning, we have $\sum_{b \in B_N} \lambda_b b = x$ for some $\lambda_b \in L$, finitely many non-zero. Then since B_L is spanning, we have $\sum_{a \in B_L} \mu_{a,b} a = \lambda_b$ for each $b \in N_B$, where $\mu_{a,b} \in K$, finitely many non-zero. So $\sum_{(a,b) \in B_L \times B_N} \mu_{a,b} ab = x$ as desired. □

> *Example.*
> *Now we can show* $\omega \notin \mathbb{Q}(\alpha_0)$ *from the previous section. We have* $3 = [\mathbb{Q}(\alpha_0) : \mathbb{Q}] = [\mathbb{Q}(\alpha_0) : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha_0) : \mathbb{Q}(\omega)]2$ *which is a contradiction because 2 does not divide 3.*

> **Definition**
>
> Let $K \to L$ be a field extension. For $A \subseteq L$, define $K(A) \subseteq L$ as the smallest subfield of L containing the image of K and A. We say $K \to L$ is finite type when there exists finite $A \subseteq L$ with $L = K(A)$. In the case of $A = \{a\}$, we write $K(a)$. We call extensions of the form $K \to K(a)$ simple.

> Given $a \in L$, one can consider the evaluation ring morphism
>
> $$\mathrm{ev}_a : K[T] \to L, f(T) \mapsto f(a)$$
>
> We say a is *algebraic over* K when there exists a non-zero f with $f(a) = 0$, i.e. $0 \neq \ker \mathrm{ev}_a$.
>
> We say $K \to L$ is algebraic when all $a \in L$ is algebraic over K.

> **Proposition – Characteristization of finite simple extensions**
> Let $K \to L$ be an extension and $a \in L$. Then the following are equivalent :
>
> 1. a is algebraic over K
> 2. $[K(a) : K]$ is finite
> 3. $K \to K(a)$ is algebraic.

Proof. $(1 \Rightarrow 2)$ We saw in section 1 how to compute $K(a)$. Specifically, consider the evaluation map $K[T] \to L, f \mapsto f(a)$ and let $K[a]$ be its image. By assumption, there exists non-zero $f \in K[T]$ with $f(a) = 0$. WLOG $\deg f = N \geq 0$. Then $1, a, \dots, a^{N-1}$ is a K-spanning set for $K[a]$. This implies $K[a]$ is a finite dimensional K-vector space and hence a field and hence $K[a] = K(a)$.

$(2 \Rightarrow 3)$ Let $b \in K(a)$. Since $[K(a) : K]$ is finite, there exists a non-trivial linear combination $0 = \sum_{n \geq 0} \lambda_n b^n$ with $\lambda_n \in K$, which implies b is algebraic over K.

$(3 \Rightarrow 1)$ trivial. ☐

> **Proposition – Characteristization of finite extensions**
> Let $K \to L$ be an extension. The following are equivalent :
>
> 1. $[L : K]$ is finite
> 2. $K \to L$ is finite type and algebraic
> 3. There exists finite $A \subseteq L$ such that $L = K(A)$ and all $a \in A$ are algebraic.

Proof. $(1 \Rightarrow 2)$ Take a K-basis and use the characterization of finite simple extensions . $(2 \Rightarrow 3)$ Clear. $(3 \Rightarrow 1)$ Induct on the size of A and use the characterization of finite simple extensions .

☐

We are now ready for the main result of this section.

> **Proposition – Embedding theorem for finite simple extensions**
> Let $K \to L$ be an extension and $a \in L$ algebraic over K. The ideal $\ker \mathrm{ev}_a \subseteq K[T]$ is generated by a unique monic polynomial. We call it the *minimal polynomial of a over K*, denoted $\min(a, K)$. Let $K \to N$ be another extension. Then we have a bijection
>
> $$\mathrm{Emb}_K(K(a), N) \simeq \{b \in N \text{ s.t. } \min(a, K) = \min(b, K)\}, \varphi \mapsto \varphi(a)$$

> In particular, $|\mathrm{Emb}_K(K(a), N)| \leq [K(a) : K]$. Elements $b \in N$ with $\min(b, K) = \min(a, K)$ are called *Galois conjugates of* a.

Proof. We saw $K(a) = K[a] \simeq K[T]/(\min(a, K))$. Given $\varphi : K(a) \to N$ a K-embedding, the composition $K[T] \to K(a) \to N$ is $\mathrm{ev}_{\varphi(a)}$. Since $K(a) \to N$ is injective, we have $\ker \mathrm{ev}_{\varphi(a)} = \ker \mathrm{ev}_a$. It follows that $\min(\varphi(a), K) = \min(a, K)$. Conversely, given $b \in N$ a Galois conjugate of a we can define the K-embedding $K(a) \simeq K[T]/(\min(a, K)) = K[T]/(\min(b, K)) \simeq K(b) \subseteq N$. ☐

We will now generalise the above to general finite extensions. For this, we need to know how embeddings from subextensions interact with the whole extension.

> **Proposition – Subextensions partition embeddings**
>
> Let $K \to L \to M$ and $K \to N$ be extensions. Then we have a bijection
>
> $$\bigsqcup_{\iota \in \mathrm{Emb}_K(L,N)} \mathrm{Emb}_L(M, N) \xrightarrow{\sim} \mathrm{Emb}_K(M, N)$$
>
> by sending $(L \to N \in \mathrm{Emb}_K(L, N), M \to N \in \mathrm{Emb}_L(M, N))$ to $M \to N$ viewed as a K-embedding.

Proof. The point is that we have a map $\mathrm{Emb}_K(M, N) \to \mathrm{Emb}_K(L, N)$ and the fibers over each $\iota : L \to N$ is precisely the set of L-embeddings $M \to N$ where N is viewed as an L-extension by $\iota : L \to N$. ☐

> **Proposition – Embedding theorem for finite extensions**
>
> Let $K \to L$ be an extension and $A \subseteq L$ finite set of algebraic generators for L over K. Let $K \to N$ be another extension and assume that for all $a \in A$ the minimal polynomial $\min(a, K)$ splits into linear factors in $N[T]$. Then
>
> $$0 < |\mathrm{Emb}_K(L, N)| \leq [L : K]$$
>
> and we have equality if for all $a \in A$ the polynomial $\min(a, K)$ has no *repeated* roots in N.

Proof. Induct on the cardinality of A. $A = \varnothing$ is trivial so let $a_0 \in A$ and $M := K(A \setminus \{a_0\})$ and assume inductively $0 < \mathrm{Emb}_K(M, N) \leq [M : K]$ with equality if all for all $a_1 \in A \setminus \{a_0\}$ we have $\min(a_1, K)$ with no repeated roots in N. Then $L = M(a_0)$. We have $\min(a_0, M)$ divides $\min(a_0, K)$ in $M[T]$, so $\min(a_0, M)$ also splits into linear factors in $N[T]$. It follows from the characterization of finite simple extensions and the tower law that

$$0 < |\mathrm{Emb}_K(L, N)| = \sum_{\mathrm{Emb}_K(M,N)} |\mathrm{Emb}_M(L, N)| \leq \sum_{\mathrm{Emb}_K(M,N)} [L : M] \leq [L : M][M : K] = [L : K]$$

Now assume all $\min(a, K)$ for $a \in A$ split into linear factors in N. This implies $\min(a_0, M)$ splits into linear factors in N so $|\mathrm{Emb}_M(L, N)| = [L : M]$. Then the first $\leq$ is an equality and the second is also by the induction hypothesis on M.

☐

3 Normal and separable extensions

Given an extension $K \to L = K(a_1, \dots, a_n)$ with a_i algebraic over K, the embedding theorem for finite extensions tells us how to construct automorphisms of L over K. For the main theorem of Galois theory to hold true, we need to have the maximum number of automorphisms, i.e. $|\mathrm{Aut}_K L| = [L : K]$. The embedding theorem indicates two ways in which this can fail :

1. the polynomials $\min(a_i, K)$ do not split into linear factors in $L[X]$
2. there exists some a_i such that $\min(a_i, K)$ has a repeated root in L.

These two phenomena are respectively called normality and separability. Let us illustrate the failure of normality by focusing on the extension $\mathbb{Q} \to \mathbb{Q}(\alpha_0)$ from the first section. Using the embedding theorem for finite simple extensions, we see that $\sigma \in \mathrm{Emb}_{\mathbb{Q}}(\mathbb{Q}(\alpha_0), \mathbb{Q}(\alpha_0))$ correspond to solutions of $T^3 - 2$ in $\mathbb{Q}(\alpha_0)$. There is only α_0: If there is another root $\tilde{\alpha_1}$ then $\tilde{\omega} := \tilde{\alpha_1}/\alpha_0$ would be a primitive cube root of unity and $[\mathbb{Q}(\tilde{\omega}) : \mathbb{Q}] = 2$ which we cannot have as we saw before. From this, we can see the problem is that $\mathbb{Q}(\alpha_0)/\mathbb{Q}$ does not contain *all* the roots of the polynomial $T^3 - 2$. More precisely, $T^3 - 2$ does not factorise into linear factors in $\mathbb{Q}(\alpha_0)[T]$. We can also see this phenomenon in the following way : there are three ways of $\mathbb{Q}$-embedding $\mathbb{Q}(\alpha_0)$ inside $\mathbb{Q}(\alpha_0, \alpha_1, \alpha_2)$ corresponding to each $\mathbb{Q}(\alpha_i)$ and their images are *different*.

> **Definition – Normal Extension**
>
> Let $K \to L$ be an extension and $f \in K[X]$. Then we say L *splits* f when f factorises into linear factors in $L[X]$.
>
> Suppose L/K is algebraic. Then it is called *normal* when for all $a \in L$, it contains all the Galois K-conjugates of a, i.e. L splits $\min(a, K)$.

> **Proposition – Splitting Polynomials**
>
> Let K be a field and $f \in K[X] \setminus K$. Then there exists an extension $K \to L$ such that f has a root in L. In particular, there exists a K-extension that splits f.

Proof. Since f is non-constant and $K[X]$ is a UFD, there exists an irreducible f_1 that divides f. Let $L = K[X]/(f_1)$. Then since f_1 is irreducible and $K[X]$ is a PID, L is a field and thus a K-extension. Note that the image of the monomial X in L is a root of f_1, and hence a root of f. To split f, use the above procedure to inductively construct a desired extension. □

> **Proposition – Characterisation of Finite Normal Extensions**
>
> Let $K \to L$ be a finite extension. Then the following are equivalent :
>
> 1. (Contains all Galois K-Conjugates) $K \to L$ normal.
> 2. (Contains all Galois K-Conjugates of Generators) There exists $A \subseteq L$ a finite set of generators of $K \to L$ such that for all $a \in A$, a is algebraic over K and L splits $\min(a, K)$.
> 3. (is a Splitting Field) There exists a polynomial $f \in K[X]$ such that L splits f and is generated by the roots of f in L.

> 4. (Image Invariance) For all extensions $K \to N$ and two $\iota_0, \iota_1 \in \mathrm{Emb}_K(L, N)$, $\iota_0 L = \iota_1 L$.

Proof. ($1 \Rightarrow 2 \Rightarrow 3$) is clear.

($3 \Rightarrow 4$) The key is that roots of f remain roots of f under K-embeddings. Let $f(X) = \prod_{k=1}^{\deg f}(X - a_k) \in L[X]$. where $a_k \in L$. Then $f(X) = \prod_{k=1}^{\deg f}(X - \iota_0(a_k)) \in N[X]$ For all a_l, since ι_1 fixes K we get

$$0 = \iota_1(f(a_l)) = f(\iota_1(a_l)) = \prod_{k=1}^{\deg f}(\iota_1(a_l) - \iota_0(a_k))$$

so there exists a_k such that $\iota_1(a_l) = \iota_0(a_k)$. Since $L = K(a_1, \ldots, a_{\deg f})$, this shows that $\iota_1 L \subseteq \iota_0 L$ and by symmetry $\iota_0 L \subseteq \iota_1 L$ as well.

($4 \Rightarrow 1$) Let $a \in L$. Since (L, ι_L) is finite, $\min(a, K)$ exists. We do not know if L splits $\min(a, K)$, but there exists an extension $L \to M$ such that M splits $\min(a, K)$. We seek to show that all Galois K-conjugates of a in M are actually in (the image of) L already. So let $\alpha \in M$ be a Galois K-conjugate of a. We have the following situation.

$$\begin{tikzcd}
K \arrow[r, "\iota_L"] & K(a) \arrow[r, "\subseteq"] \arrow[dr, "\phi_\alpha"] & L \arrow[d, "\iota_M"] \\
 & & M
\end{tikzcd}$$

By the embedding theorem for finite simple extensions, there exists $\phi_\alpha \in \mathrm{Emb}_K(K(a), M)$ that maps $a \mapsto \alpha$. Suppose we have an $\iota_1 \in \mathrm{Emb}_{K(a)}(L, \phi_\alpha)$. Then certainly $\iota_1 \in \mathrm{Emb}_K(L, \iota_M \circ \iota_L)$. Also, trivially $\iota_M \in \mathrm{Emb}_K(L, \iota_M \circ \iota_L)$. So $\iota_1 L = \iota_M L$ implies $\alpha \in \iota_M L$ as desired. It thus suffices to give an $\iota_1 \in \mathrm{Emb}_{K(a)}(L, \phi_\alpha)$. Well, since (L, ι_L) is finite, it is also a finite $K(a)$-extension, so it is generated by some finite subset B whose elements are all algebraic over $K(a)$. Then we can extend M so that it splits all $\min(b, K(a))$ for $b \in B$. Thus by the embedding theorem, we have an $\iota_1 \in \mathrm{Emb}_{K(a)}(L, \phi_\alpha)$. ☐

Now let us discuss separability. As we will see, existence of inseparable irreducible polynomials is linked with the *characteristic* of the base field K. This implies that in terms of finding an insolvable quintic over $\mathbb{Q}$, the problem of inseparable minimal polynomials never happens.

> **Definition – Separable Polynomial, Separable extension**
>
> f is said to be *separable* when for all K-extensions in which f splits, f has no repeated roots. If otherwise, f is called *inseparable*. An algebraic extension $K \to L$ is called separable when for all $a \in L$, the polynomial $\min(a, K)$ is separable.

> **Proposition – Characterization of separable polymomials using differentials**
>
> Let K be a field and $f = \sum_{0 \leq n} f_n X^n \in K[X]$. The *formal derivative of* f is defined to be $f' = \sum_{0<n} n f_n X^{n-1}$. Then f is separable iff $(f, f') = 1$.

Intuition : if $a \in K$, writing $f(X) = \sum_{d \geq 0} \lambda_d (X - a)^d$, a is a higher order root iff $\lambda_0 = \lambda_1 = 0$.

Proof. We will prove f is inseparable iff $(f, f') \neq 1$. Assume f is inseparable. Suppose $(f, f') = 1$. Then by the Euclidean algorithm there exists $\lambda, \mu \in K[X]$ such that $\lambda f + \mu f' = 1$. Let $K \to L$ be an extension where f has a repeated root a. By factoring $f(X) = (X - a)^2 g(X)$ in $L[X]$ and the product rule for formal differentiation (which can be proved by induction), we see a contradiction

$$1 = \lambda(a)f(a) + \mu(a)f'(a) = 0 + 0 = 0$$

Now assume $(f, f') \neq 1$. Let $h \in K[X]$ be the GCD of f and f', which is non-constant by assumption. Let $K \to L$ be any extension that splits f. It also splits h. Let $a \in L$ with $h(a) = 0$. We can write $f(X) = (X - a)^d g(X)$ in $L[X]$ for some $d \geq 0$ and $g(a) \neq 0$. Since h divides f we have $f(a) = 0$ so $d \geq 1$. Suppose $d = 1$. We also have h divides f' yielding a contradiction

$$0 = f'(a) = g(a) \neq 0$$

☐

To give an example of an inseparable extension, we need to discuss the notion of the characteristic of a field.

> **Definition – Characteristic of a Field**
>
> Let K be a field. $\mathbb{Z}$ is generated by 1 and ring morphisms must preserve 1, so there is a unique ring morphism $\mathbb{Z} \to K$. Its image is an ID since K is an ID. So by $\mathbb{Z}$ PID, its kernel is generated by either zero or a (positive) prime. This is defined as the *characteristic of K*, denoted $\mathrm{Char} K$.
>
> More generally, the characteristic of any integral domain A is defined in the same way.

> *Example.*
> *All fields K of characteristic 0 have a unique extension map $\mathbb{Q} \to K$. Similarly, all fields K of characteristic $p > 0$ have a unique extension map $\mathbb{F}_p \to K$.*

The following is the root of all interesting phenomena in positive characteristic.

> **Proposition – Freshman's dream**
>
> Let A be an $\mathbb{F}_p$-algebra, i.e. $p = 0$ in A, and $a, b \in A$. Then $(a + b)^p = a^p + b^p$

Proof. The point is that the binomial coefficient $\binom{p}{k}$ for $0 < k < p$ is divisible by p. ☐

> *Example.*
> *Consider $K = \mathbb{F}_p(T) := \mathrm{Frac}\, \mathbb{F}_p[T]$ and the polynomial $f(X) = X^p - T \in K[X]$. Then by Eisenstein's criterion f is irreducible. Let $L := K[X]/(f)$ and $T^{1/p}$ the image of X in L. Then in $L[X]$ we have by Freshman's dream*
>
> $$f(X) = X^p - T = X^p - (T^{1/p})^p = (X - T^{1/p})^p$$
>
> *So f is inseparable. Notice in that $f' = 0$ so indeed $(f, f') \neq 1$.*

In fact, we cannot have inseparable extensions in characteristic zero.

> **Proposition**
> Let K be characteristic zero. Then any irreducible $f \in K[T]$ is separable.

Proof. f' is either zero or has degree strictly less than f. WLOG f is monic. Then $0 = f'$ implies by looking at the leading coefficient, $0 = \deg f$ as elements of K, contradicting the characteristic of K being zero. So $f' \neq 0$. But then we must have $(f, f') = 1$ because $\deg f' < \deg f$ implies f cannot divide f'. $\square$

4 Galois extensions and the correspondence

> **Definition**
> An extension $K \to L$ is called finite Galois when there exists a finite subgroup $G \subseteq \operatorname{Aut}_K L$ such that $K = L^G$.

The following is arguably the fundamental theorem of Galois theory.

> **Proposition – Artin's characterization of finite Galois extensions**
> Let $K \to L$ be an extension. Then $K \to L$ is finite, normal, separable iff $K \to L$ is finite Galois. In this case the finite subgroup $G \subseteq \operatorname{Aut}_K L$ such that $K = L^G$ must be $\operatorname{Aut}_K L$.

Proof. Slogan : *set of Galois conjugates = orbit*.

($1 \Rightarrow 2$) By the embedding theorem, $|\operatorname{Aut}_K L| \leq [L : K]$. We claim that $G := \operatorname{Aut}_K L$ works. Let $a \in L^G$. Goal : $a \in K$. It suffices to show $\min(a, K)$ is linear. Since $K \to L$ is normal, $\min(a, K)$ splits in L. Since $K \to L$ is separable, it suffices to show that for any Galois K-conjugate α of a we have $\alpha = a$. Let $\alpha \in L$ with $\min(a, K)(\alpha) = 0$. Since $a \in L^G$ is suffices to give $\sigma \in \operatorname{Aut}_K L$ which $\sigma(a) = \alpha$. By the embedding theorem applied to $K(a) \to L$, we can extend $K(a) \simeq K(\alpha) \to L$ to an automorphism $\sigma : L \to L$ preserving K. This maps a to α as desired.

($2 \Rightarrow 1$) Let G be a finite subgroup of $\operatorname{Aut}_K L$ such that $K = L^G$. For $a \in L$ we claim that

$$\min(a, K)(T) = \prod_{\alpha \in Ga} (T - \alpha) \in L[T]$$

where Ga denotes the G-orbit of a. This proves that L/K is normal and separable. Let $f \in L[T]$ be the above product. The claim is equivalent to showing $f \in L^G[T] = K[T]$ and f is irreducible in $K[T]$. Let $\sigma \in G$. Then

$$\sigma f(T) = \sigma \prod_{\alpha \in Ga} (T - \alpha) = \prod_{\alpha \in Ga} (T - \sigma(\alpha)) = \prod_{\tilde{\alpha} \in Ga} (T - \tilde{\alpha}) = f(T)$$

Therefore $f \in K[T]$. For irreducibility, if $f = gh$ is a non-trivial factoring in $K[T]$ then one of g or h has a as a root. Say it's g, then by applying $\sigma \in G$ to the equation $0 = g(a)$ we get that g has all $\alpha \in Ga$ as roots, i.e. f divides g, a contradiction.

Now we show L/K is finite. We are expecting $G = \operatorname{Aut}_K L$ which should have size $[L : K]$. So we will bound $[L : K] \leq |G|$. Magic claim : $\dim_K L = \dim_L L[G] = |G|$ where $L[G]$ is the set of functions from G to L. It will suffice for us to show that any K-linearly independent set gives rise to a L-linearly independent set in $L[G]$ with the same cardinality. Let $A \subseteq L$ be a finite K-linearly independent set. Define $\tilde{A} := \{\operatorname{ev}_a\}_{a \in A} \subseteq L[G]$.

Then $\mathrm{ev}\_ : A \to \tilde{A}$ is a bijection because $\mathrm{ev}_a = \mathrm{ev}_{a_1}$ implies $a = \mathrm{ev}_a(e) = \mathrm{ev}_{a_1}(e) = a_1$ and surjectivity is by definition. Claim : $\tilde{A}$ is a L-linearly independent set in $L[G]$. We induct on $|A|$. Let $\sum_{x \in X_0} \lambda_x ev_x = 0$ with $\lambda_x \in L$. Suppose for a contradiction that there exists $a_0 \in A$ such that $\lambda_{a_0} \neq 0$. It suffices to show for all $a \in A$ we have $\lambda_a \in L^G = K$, for then by evaluating at $e \in G$ gives $0 = \sum_{a \in A} \lambda_a a$, implying all $\lambda_a = 0$. So let $\sigma \in G$ with the goal of showing $\sigma(\lambda_a) = \lambda_a$ for all $a \in A$. By rescaling, WLOG $\lambda_{a_0} = 1$. By induction it suffices to show

$$\sum_{x \in X_0 \setminus \{x_0\}} (\lambda_x - \sigma(\lambda_x)) ev_x = 0 \in L[G]$$

Let $\rho \in G$. Then we have as desired

$$\begin{aligned} \sum_{a \in A \setminus \{a_0\}} (\lambda_a - \sigma(\lambda_a)) ev_a(\rho) &= \sum_{x \in X_0} \lambda_x ev_x(\rho) - \sum_{a \in A} \sigma(\lambda_a) \rho(a) \\ = -\sigma \left(\sum_{a \in A} \lambda_a \sigma^{-1} \rho(a) \right) &= -\sigma \left(\left(\sum_{a \in A} \lambda_a \, \mathrm{ev}_a \right) \sigma^{-1} \rho \right) = 0 \end{aligned}$$

□

> **Proposition – The Galois correspondence**
> Let $K \to L$ be a Galois extension of fields and let $G := \mathrm{Aut}_K L$. Then we have an order reversing bijection
>
> $$\begin{tikzcd} \{K\text{-subextensions } E \subseteq L\} \arrow[r, shift left=1.5, "\mathrm{Aut}\_L"] \arrow[r, phantom, "\simeq"] & \{\text{subgroups of } \mathrm{Aut}_K L\} \arrow[l, shift left=1.5, "L^{-}"] \end{tikzcd}$$
>
> Furthermore, for $E \subseteq L$ a K-subextension we have the following :
>
> 1. (Degree equals Index) $[E : K] = [\mathrm{Aut}_K L : \mathrm{Aut}_E L]$.
> 2. (Group Action) For all $\sigma \in \mathrm{Aut}_K L$, $\mathrm{Aut}_{\sigma E} L = \sigma \, \mathrm{Aut}_E L \sigma^{-1}$.
> 3. (Normality) E is a normal K-extension if and only if $\mathrm{Aut}_E L$ is a normal subgroup of $\mathrm{Aut}_K L$. In this case, we have the isomorphism $\mathrm{Aut}_K E \cong \mathrm{Aut}_K L / \mathrm{Aut}_E L$.

Proof. We need a lemma.

> *Lemma. Let $K \to E \to L$ be a sequence of extensions.*
>
> 1. *If $K \to L$ is finite normal, then $E \to L$ is finite normal.*
> 2. *If $K \to L$ is finite separable, then $E \to L$ is finite separable.*
>
> *Proof.* Exercise. ■

(Surjectivity) Let $H \subseteq \mathrm{Aut}_K L$ be a subgroup. Then $\mathrm{Aut}_{L^H} L = H$ by the characterisation of Galois extensions. Now let $E \subseteq L$ be a K-subextension. Then by the above lemma, L/E is Galois so $E = L^{\mathrm{Aut}_E L}$.

(Injectivity) This actually does not use any Galois theory and is true for any partially ordered set. Here is the statement.

> *Lemma. Let I, J be partially ordered sets, $F : I \to J$ and $G : J \to I$ be order reversing functions satisfying:*
>
> - *(Adjunction) For all $x \in I$ and $y \in J$, $x \leq G(y)$ iff $y \leq F(x)$.*
>
> *Then $FGF = F$ and $GFG = G$. In particular, F and G induce a bijection on the images FI, GJ.*
>
> *Proof.* Exercise. ■

(Degree equals index) Use the above lemma and the characterisation of Galois extensions.

(Group action) Exercise.

(Normality) If E/K is normal, then image-invariance of normal extensions we get a well-defined morphism of groups by restriction

$$\operatorname{Aut}_K L \to \operatorname{Aut}_K E$$

The kernel is by definition $\operatorname{Aut}_E L$ so it is normal.

If $\operatorname{Aut}_E L$ is normal, then for any $\sigma \in \operatorname{Aut}_K L$ we have

$$\sigma E = L^{\operatorname{Aut}_{\sigma E} L} = L^{\sigma \operatorname{Aut}_E L \sigma^{-1}} = L^{\operatorname{Aut}_E L} = E$$

so restriction gives a well-defined morphism of groups $\operatorname{Aut}_K L \to \operatorname{Aut}_K E$. Let G be the image. Then $E^G = E \cap L^{\operatorname{Aut}_K L} = E \cap L^G = E \cap K = K$ so E/K is Galois and hence normal. By the characterisation of Galois extensions, G must be all of $\operatorname{Aut}_K E$ and hence by the first isomorphism theorem of groups we have $\operatorname{Aut}_K E \simeq \operatorname{Aut}_K L / \operatorname{Aut}_E L$.

□

> *Example.*
> *Let us compute the Galois group of $T^4 - a \in \mathbb{Q}[T]$ over $K = \mathbb{Q}$ where a is a positive integer with no square factors.*
>
> *Let $p > 0$ be a prime that divides a. Then $T^4 - a$ satisfies Eisenstein's criterion and hence is irreducible in $\mathbb{Q}[T]$. Let L/K be a splitting field of $T^4 - a$ and $\alpha \in L$ any root. This is a Galois extension because $\mathbb{Q}$ is characteristic zero. By separability of $T^4 - a$, there exists another root β not equal to $\pm\alpha$. Let $i := \beta/\alpha$. Then $0 = i^4 - 1 = (i-1)(i+1)(i^2+1)$ implies $i^2 + 1 = 0$. So the four roots are $\alpha, \alpha i, \alpha i^2, \alpha i^3$.*
>
> *Let $\sqrt[4]{2} \in \mathbb{R}$ be the unique positive fourth-root of 2. Using the embedding theorem, there exists an embedding $\phi : L \to \mathbb{C}$ such that $\phi(\alpha) = \sqrt[4]{2}$. From this, we deduce $i \notin \mathbb{Q}(\alpha)$ because if it were it would give an element $\phi(i) \in \phi\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ which is not fixed by complex conjugation. It follows that $T^2 + 1$ is irreducible in $\mathbb{Q}(\alpha)[T]$ and hence $[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$.* [a]
>
> *Using embedding theorem for $L/\mathbb{Q}(\alpha)$, we get $\tau \in \operatorname{Aut}_{\mathbb{Q}} L$ such that*
>
> $$\tau(i) = -i \qquad\qquad \tau(\alpha) = \alpha$$
>
> *Since $\deg \min(\alpha, \mathbb{Q}(i)) = [L : \mathbb{Q}(i)] = 4$ by the tower law, we have $\min(\alpha, \mathbb{Q}(i)) = T^4 - 2$. Using embedding*

theorem again, we have $\sigma \in \operatorname{Aut}_{\mathbb{Q}} L$ such that

$$\sigma(i) = i \qquad\qquad \sigma(\alpha) = \alpha i$$

We have $\sigma^k(\alpha) = \alpha i^k$ so σ has order 4.

$$\tau\sigma\tau^{-1}(i) = \tau\sigma(-i) = \tau(-i) = i$$
$$\tau\sigma\tau^{-1}(\alpha) = \tau\sigma(\alpha) = \tau(\alpha i) = -\alpha i = \sigma^{-1}(\alpha)$$

So $\tau\sigma\tau^{-1} = \sigma^{-1}$ and thus $\operatorname{Aut}_{\mathbb{Q}} L \simeq D_8$. We have the following classification of subgroups of D_8

$$\begin{tikzcd}
 & & \langle 1 \rangle \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
\langle \tau \rangle \arrow[dr] & \langle \tau\sigma^2 \rangle \arrow[d] & \langle \sigma^2 \rangle \arrow[dl] \arrow[d] \arrow[dr] & \langle \tau\sigma \rangle \arrow[d] & \langle \tau\sigma^3 \rangle \arrow[dl] \\
 & \langle \tau, \sigma^2 \rangle \arrow[dr] & \langle \sigma \rangle \arrow[d] & \langle \tau\sigma, \sigma^2 \rangle \arrow[dl] & \\
 & & \langle \sigma, \tau \rangle & &
\end{tikzcd}$$

The corresponding intermediate extensions are :

$$\begin{tikzcd}
 & & \mathbb{Q}(\alpha, i) & & \\
\mathbb{Q}(\alpha) \arrow[urr] & \mathbb{Q}(\alpha i) \arrow[ur] & \mathbb{Q}(i, \alpha^2) \arrow[u] & \mathbb{Q}(\alpha - i\alpha) \arrow[ul] & \mathbb{Q}(\alpha + i\alpha) \arrow[ull] \\
 & \mathbb{Q}(\alpha^2) \arrow[ul] \arrow[u] \arrow[ur] & \mathbb{Q}(i) \arrow[u] & \mathbb{Q}(i\alpha^2) \arrow[ul] \arrow[u] \arrow[ur] & \\
 & & \mathbb{Q} \arrow[ul] \arrow[u] \arrow[ur] & &
\end{tikzcd}$$

To compute fixed subfields L^H of a given subgroup H of $\operatorname{Aut}_{\mathbb{Q}} L$, one can use linear algebra: Choose a $\mathbb{Q}$-basis for L, for each $\sigma \in H$ write the matrix A given by the K-linear map $x \mapsto \sigma(x)$ and compute the kernel of $A - I$ where I is the identity matrix. Alternatively, one can check that it is invariant and then check the degree. For example, $\tau\sigma(\alpha - i\alpha) = \tau(\alpha i + \alpha) = \alpha - \alpha i$ so $\mathbb{Q}(\alpha - i\alpha) \subseteq L^{\langle \tau\sigma \rangle}$.

$$(\alpha - i\alpha)^4 = (-2i\alpha^2)^2 = -4a$$

> *so* $[\mathbb{Q}(\alpha - i\alpha) : \mathbb{Q}] \leq 4$. *On the other hand, if* $i \in \mathbb{Q}(\alpha - i\alpha)$ *then* $\alpha = (\alpha - i\alpha + i(\alpha - i\alpha))/2$ *implies* $L = \mathbb{Q}(\alpha - i\alpha)$ *which would imply* $8 = [L : \mathbb{Q}] \leq 4$ *a contradiction. Therefore* $[L : \mathbb{Q}(\alpha - i\alpha)] = 2$ *and hence* $[\mathbb{Q}(\alpha - i\alpha) : \mathbb{Q}] = 4$. *Since* $[L^{\langle \tau\sigma \rangle} : \mathbb{Q}] = [\langle \sigma, \tau \rangle : \langle \tau\sigma \rangle] = 4$ *we conclude* $\mathbb{Q}(\alpha - i\alpha) = L^{\langle \tau\sigma \rangle}$.
>
> ---
>
> [a] There should be a way to do this without using $\mathbb{R}$ but this is probably the easiest way.

5 Cyclotomic extensions, Cyclic extensions

We saw in the example of $T^3 - 2$ that in understanding its roots, the roots of $T^3 - 1$ appeared. This reduces the understanding of radical Galois extensions into two steps : *cyclotomic* and *cyclic* extensions. We study these as stepping stones towards understanding radical extensions.

> **Definition**
>
> Let K be a field and $f \in K[T]$. A *splitting field of* f is an extension $K \to L$ that splits f and is generated by the roots of f.

It will be useful to have another characterisation of Galois extensions.

> **Proposition – Splitting field characterisation of Galois extensions**
>
> Let $K \to L$ be an extension. Then L/K is the splitting field of a separable $f \in K[T]$ iff L/K is Galois.

Proof. ($\Rightarrow$) Let $G = \mathrm{Aut}_K L$ which is finite by the embedding theorem. We know that L/L^G is Galois so STS $L^G = K$. Since f is separable, $\min(\alpha, K)$ is also separable for any root α of f. Since the roots of f generate L over K, by the embedding theorem we have $|G| = [L : K]$. Then $[L^G : K] = [L : K]/[L : L^G] = [L : K]/[L : K] = 1$.

($\Leftarrow$) By the characterisation of normal extensions, L/K is the splitting field of some $f \in K[T]$. Remove all repeated irreducible factors of f so that f is square-free. Any pair of distinct irreducible factors g, h of f must satisfy $1 = \lambda g + \mu h$ for some $\lambda, \mu \in K[T]$. It follows that they do not share roots in any extension of K. The irreducible factors of f are (scalar multiplies of) minimal polynomials, which are separable because L/K is Galois. Thus f is a separable polynomial. □

> **Proposition – Galois groups of cyclotomic extensions**
>
> Let $n \in \mathbb{N}$ and L/K the splitting field of $X^n - 1 \in K[T]$. Assume that $X^n - 1$ is separable, or equivalently $n \neq 0$ as elements of K. Let $\mu_n \subseteq L^\times$ be the subgroup of roots of $X^n - 1$. A *primitive* n*-th root of unity* is defined as a generator of μ_n. Then
>
> 1. there are $\phi(n)$ many primitive n-th roots of unity in L
> 2. the group morphism
>
> $$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\times &\to \mathrm{Aut}_{\mathrm{Grp}}\, \mu_n \\ k &\mapsto (z \mapsto z^k) \end{aligned}$$

> is an isomorphism, where $\operatorname{Aut}_{\mathrm{Grp}} \mu_n$ denotes the group of group automorphisms of μ_n. The restriction $\operatorname{Gal}(L/K) \to \operatorname{Aut}_{\mathrm{Grp}} \mu_n$ is injective, so $\operatorname{Gal}(L/K)$ is abelian.

Proof. (1) Let $\mu_n^d \subseteq \mu_n$ be the subset of elements with order d. Then by strong induction on n we have[1]

$$|\mu_n^n| = |\mu_n| - \sum_{n>d|n} \left|\mu_n^d\right| n - \sum_{n>d|n} \phi(d) = \phi(n)$$

(2) Being a splitting field of a separable polynomial, it makes sense to talk about the Galois group L/K. We give an inverse group morphism. Since $\phi(n) > 0$ there exists $z_0 \in \mu_n$ with order n. For any $\sigma \in \operatorname{Aut}_{\mathrm{Grp}} \mu_n$, there is a unique $k_\sigma \in \mathbb{Z}/n\mathbb{Z}$ such that $\sigma(z_0) = z_0^{k_\sigma}$. Since σ has to send z_0 to another element of order n, we must have $(n, k_\sigma) = 1$ i.e. $k_\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\sigma \mapsto k_\sigma$ gives the desired inverse.[2] ☐

Remark. It is possible to show that when $K = \mathbb{Q}$, the morphism $\operatorname{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \to \operatorname{Aut}_{\mathrm{Grp}} \mu_n$ is surjective and hence bijective. This is not necessary for solvability of polynomials so we will return to this later.

> **Proposition – Characterization of cyclic extensions**
> Let $n \in \mathbb{Z}_{>0}$ and $K \to L$ be an extension where $T^n - 1 \in K[T]$ is split and separable in K. Then
>
> 1. if $L = K(\alpha)$ where $\alpha^n \in K$ and is the minimal power of α in K, then L/K is Galois and the map
>
> $$\begin{aligned} \operatorname{Gal}(L/K) &\to \mu_n \\ \sigma &\mapsto \sigma(\alpha)/\alpha \end{aligned}$$
>
>   is group isomorphism. Hence $\operatorname{Gal}(L/K)$ is cyclic.
> 2. Conversely if L/K is Galois with $\operatorname{Gal}(L/K)$ cyclic order n then there exists $\alpha \in L$ such that $L = K(\alpha)$ and α^n is the minimal power of α in K.

This is completely analogous to the situation $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\omega)$.

Proof. (1) (Galois) L/K is the splitting field of $T^n - \alpha^n$ which is separable by separability of $T^n - 1$.

(Group morphism) For $\sigma, \rho \in \operatorname{Gal}(L/K)$ we have

$$\frac{\sigma(\rho(\alpha))}{\alpha} = \frac{\sigma(\rho(\alpha))}{\rho(\alpha)} \frac{\rho(\alpha)}{\alpha} = \frac{\sigma(\alpha)}{\alpha} \frac{\rho(\alpha)}{\alpha}$$

because $\rho(\alpha) = \alpha z$ for some $z \in \mu_n$ so

$$\frac{\sigma(\rho(\alpha))}{\rho(\alpha)} = \frac{\sigma(\alpha) z}{\alpha z} = \frac{\sigma(\alpha)}{\alpha}$$

---

[1] Here is a proof of $n = \sum_{0 \leq d|n} \phi(d)$. We take as definition $\phi(d) := \left|(\mathbb{Z}/d\mathbb{Z})^\times\right|$. Then the chinese remainder theorem implies ϕ is multiplicative so it suffices to prove the result for $n = p^a$ where $p > 0$ is prime and $a > 0$. Now $p^a = (p^a - p^{a-1}) + \cdots + (p-1) + 1 = \phi(p^a) + \phi(p^{a-1}) + \cdots + \phi(p) + 1$ because an element in $\mathbb{Z}/p^k\mathbb{Z}$ is invertible iff it is invertible mod p.

[2] Although the definition of the inverse used a choice of generator of μ_n, it is independent of this choice because inverse of group morphisms are unique and $(\mathbb{Z}/n\mathbb{Z})^\times \to \operatorname{Aut}_{\mathrm{Grp}} \mu_n$ does not use any choices of generator of μ_n.

(Bijective) Injectivity follows from kernel being trivial because any σ is determined by what it does on α. Suppose for a contradiction that $\mathrm{Gal}(L/K) \to \mu_n$ is not surjective. Then the image of $\mathrm{Gal}(L/K)$ is a subgroup of order $d < n$ so by Lagrange's theorem for all $\sigma \in \mathrm{Gal}(L/K)$ we have $(\sigma(\alpha)/\alpha)^d = 1$. This says $\sigma(\alpha^d) = \alpha^d$ i.e. $\alpha^d \in L^G = K$ which contradicts minimality of n.

(2) Let $\sigma \in \mathrm{Gal}(L/K)$ be a generator. The proof of (1) shows that we are expecting $\alpha \in L$ to be such that $\sigma(\alpha)/\alpha \in \mu_n$, i.e. α is an eigenvector of σ with eigenvalue $z \in \mu_n$. So consider σ as a K-linear map $L \to L$. Then the minimal polynomial of σ divides $T^n - 1$ in $K[T]$. This is split and separable over K so the minimal polynomial of σ is split and separable over K. This occurs iff σ is diagonalizable as a K-linear map. The eigenvalues of σ are precisely the roots of its minimal polynomial, which divides $T^n - 1$ so consequently there exists $\alpha \in L$ with eigenvalue $z \in \mu_n$, i.e. $\sigma(\alpha) = z\alpha$. Then $\sigma((\alpha)^n) = (\sigma(\alpha))^n = (z\alpha)^n = \alpha^n$ so $\alpha^n \in L^G = K$. Let $\tilde{n}$ be the minimal power of α in K. Then by (1) we have $\tilde{n} = |\mathrm{Gal}(L/K)| = n$. ☐

6 Radical extensions

Today we discuss solvability polynomials.

> **Definition**
>
> Let $K \to L$ be an extension. We say it is *radical* when there exists a chain of subextensions
>
> $$K = L_0 \to L_1 \to \cdots \to L_{n-1} \to L_n = L$$
>
> such that each $L_{i+1} = L_i(\alpha_i)$ for some α_i with $\alpha_i^{d_i} \in L_i$ for some $d_i > 0$.
>
> For $f \in K[T]$ we say f is *solvable by radicals* when there exists a radical extension L/K which splits f.

Some group theoretic things we need...

> **Definition**
>
> Let G be a finite group. Then G is called solvable when there exists a chain
>
> $$1 = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n = G$$
>
> such that H_{n+1}/H_n is cyclic.

> **Proposition**
>
> Suppose we have a normal subgroup N of a finite group G.
>
> $$1 \to N \to G \to G/N \to 1$$
>
> If N and G/N are solvable, then G is solvable. If G is solvable, then N is solvable. [a]
>
> ---
>
> [a] One can prove in this case that G/N is solvable, too, but this is not relevant for solvability of polynomials.

Proof. Exercise in group theory. ☐

The main result is :

> **Proposition – Characterization of solvable polynomials in characteristic zero**
> Let K be a characteristic zero field and $f \in K[T]$ be irreducible. Then f is solvable by radicals iff there exists a splitting field L/K of f such that $\mathrm{Gal}(L/K)$ is solvable.

Remark. In the above, L/K is normal by the characterization of finite normal extensions. K characteristic zero implies all extensions of K are separable, so L/K is indeed Galois and it makes sense to talk about its Galois group. Furthemore if $\tilde{L}/K$ is another splitting field of f then by the embedding theorem there exists an isomorphism $\gamma : L \simeq \tilde{L}$ of extensions of K. It follows that $\gamma\_\gamma^{-1} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(\tilde{L}/K)$ is an isomorphism of groups.[1] So for a polynomial f solvable by radicals, *all* splitting fields of f have solvable Galois groups.

Proof of characterization of solvable polynomials in characteristic zero. ($\Rightarrow$) Assume there is a tower of simple radical extensions

$$K = L_0 \to L_1 \to \cdots \to L_{n-1} \to L_n = L$$

where $L_{i+1} = L_i(\alpha_i)$ for some $\alpha_i^{d_i} \in L_i$ and $d_i > 0$, and that L contains a splitting field of f. **Let us first assume L/K is Galois.** Then L/K Galois implies it splits $X^N - 1$ where $N = d_1 \cdots d_n$. It is separable by the assumption that K is characteristic zero. Let $\tilde{L}_0 := L_0(\mu_N)$ and $\tilde{L}_{i+1} := \tilde{L}_i(\alpha_i)$.

$$\begin{tikzcd}
L_0 \arrow[r] \arrow[d] & L_1 \arrow[r] \arrow[d] & \cdots \arrow[r] \arrow[d] & L_{n-1} \arrow[r] \arrow[d] & L_n = L \arrow[d, "="] \\
\tilde{L}_0 \arrow[r] & \tilde{L}_1 \arrow[r] & \cdots \arrow[r] & \tilde{L}_{n-1} \arrow[r] & \tilde{L}_n = L
\end{tikzcd}$$

Applying the main theorem of Galois theory we obtain a sequence of subgroups

$$\mathrm{Gal}(\tilde{L}_n/\tilde{L}_n) \subseteq \mathrm{Gal}(\tilde{L}_n/\tilde{L}_{n-1}) \subseteq \cdots \subseteq \mathrm{Gal}(\tilde{L}_n/\tilde{L}_1) \subseteq \mathrm{Gal}(\tilde{L}_n/\tilde{L}_0) \subseteq \mathrm{Gal}(\tilde{L}_n/L_0) = \mathrm{Gal}(L/K)$$

Then

1. each factor group $\mathrm{Gal}(\tilde{L}_n/\tilde{L}_i)/\mathrm{Gal}(\tilde{L}_n/\tilde{L}_i) \simeq \mathrm{Gal}(\tilde{L}_{i+1}/\tilde{L}_i)$ is cyclic by the characterisation of cyclic extensions.
2. For the final factor group at the top, $\tilde{L}_0/L_0$ is a cyclotomic extension. So it has abelian Galois group, which is in particular solvable by, say, the classification of finite abelian groups.

Thus $\mathrm{Gal}(L/K)$ is solvable.

To complete the proof of the forward direction, we need to show that we can always enlarge L so that L/K is not just radical but also Galois. By splitting minimal polynomials of generators of L/K, we can find N/L such that N/K is finite normal. Since K is characteristic zero, N/K is separable and hence Galois. But N is made with choices (the generators of L/K) so we do not know immediately that N/K is radical.

---

[1] This is analogous to the following phenomenon from algebraic topology : given a topological space X and a path γ from a point x to $\tilde{x}$, then γ_γ^{-1} gives an isomorphism $\pi_1(X, x) \simeq \pi_1(X, \tilde{x})$. These two are united in *algebraic geometry*.

Let $\mathrm{Gal}(N/K) = \{\sigma_1, \dots, \sigma_{[N:K]}\}$ with $\sigma_1 = e$. The reason why L/K is not Galois is more or less because we don't have the Galois conjugates of α_i. So we add them in. Define the tower of subextensions

$$\begin{aligned} K = L_{1,0} &\subseteq L_{1,1} \subseteq \cdots \subseteq L_{1,n-1} \subseteq L_{1,n} \\ &= L_{2,0} \subseteq L_{2,1} \subseteq \cdots \subseteq L_{2,n-1} \subseteq L_{2,n} \\ &= L_{3,0} \subseteq \cdots \\ &= L_{[N:K],0} \subseteq L_{[N:K],1} \subseteq \cdots \subseteq L_{[N:K],n} =: M \end{aligned}$$

where $L_{i,j+1} = L_{i,j}(\sigma_i(\alpha_j))$. Goal : each step is simple radical and M/K is Galois. The point is that

- $\sigma_2 L_{1,1} = \sigma_2 L_{1,0}(\alpha_1) = L_{1,0}(\sigma_2(\alpha_1)) \subseteq L_{2,0}(\sigma_2(\alpha_1)) = L_{2,1}$
- $\sigma_2 L_{1,2} = \sigma_2 L_{1,1}(\alpha_2) \subseteq L_{2,1}(\sigma_2(\alpha_2)) = L_{2,2}$
- by induction the same for the entirety of second row.
- By the same reasoning, we get for every i-th row $\sigma_i L_{1,j} \subseteq L_{i,j}$ for all j.

From this we get

$$(\sigma_i(\alpha_j))^{d_j} = \sigma_i(\alpha_j^{d_j}) \in L_{i,j}$$

so that $L_{i,j+1}/L_{i,j}$ is simple radical. To show M/K is Galois, it suffices by the characterisation of Galois extensions to show that M is stable under the action of $\mathrm{Gal}(N/K)$. For this we guess another construction of M. From the proof of the Tower law, we define $\tilde{M}$ as the set of finite K-linear combinations of $\sigma_1(x_1) \cdots \sigma_{[N:K]}(x_{[N:K]})$ where $x_i \in L$. This is a subring of N containing K and finiteness of L/K implies finiteness of $\tilde{M}$ as a K-vector space. It follows that $\tilde{M}$ is a K-subextension of N/K. By looking at the proof of the Tower law, $M \subseteq \tilde{M}$. Conversely, any $\sigma_1(x_1) \cdots \sigma_{[N:K]}(x_{[N:K]}) \in (\sigma_1 L) \cdots (\sigma_{[N:K]} L) \subseteq L_{1,n} \cdots L_{[N:K],n} \subseteq M$ so $\tilde{M} \subseteq M$ and hence $M = \tilde{M}$. [1]

($\Leftarrow$) Suppose L/K is a splitting field of f and $\mathrm{Gal}(L/K)$ is solvable. Again, for the characterisation of cyclic extensions to apply we need enough roots of unity in our base field. Let $L \to \tilde{L}$ be a splitting field of $T^{[L:K]} - 1 \in L[T]$ and $\tilde{K} := K(\mu_{[L:K]}) \subseteq \tilde{L}$. The extension $\tilde{L}/K$ is the splitting field of $(T^{[L:K]} - 1)f \in K[T]$, and hence Galois because we are in characteristic zero. By the main theorem of Galois theory, we have

$$\mathrm{Gal}(\tilde{L}/K)/\,\mathrm{Gal}(\tilde{L}/L) \simeq \mathrm{Gal}(L/K)$$

The latter is solvable and the kernel is solvable too because $\tilde{L}/L$ is a cyclotomic extension. Thus $\mathrm{Gal}\,\tilde{L}/K$ is also solvable. Since $\mathrm{Gal}\,\tilde{L}/\tilde{K}$ is a normal subgroup, it is also solvable. So we have

$$1 = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_{n-1} \triangleleft H_n = \mathrm{Gal}(\tilde{L}/\tilde{K})$$

with cyclic factor groups. To apply the characterisation of cyclic extensions to get $\tilde{K} \to \tilde{L}$, we need to know $|H_{i+1}/H_i|$ divide $[L : K]$ so that we have the correct roots of unity. $|H_{i+1}/H_i|$ divides $\left|\mathrm{Gal}(\tilde{L}/\tilde{K})\right|$ so it STS that the composition

$$\mathrm{Gal}\,\tilde{L}/\tilde{K} \to \mathrm{Gal}(\tilde{L}/K) \to \mathrm{Gal}\,L/K$$

is injective. If $\sigma \in \mathrm{Gal}(\tilde{L}/\tilde{K})$ fixes L then it fixes the roots of f and $T^n - 1$. But these generate $\tilde{L}$ over K so then $\sigma = 1$. Hence, $\tilde{K} \to \tilde{L}$ is radical. Since $K \to \tilde{K}$ is cyclotomic and so also radical, we have thus that $K \to \tilde{L}$ is radical, completing the proof. □

---

[1] The trick of constructing $\tilde{M}$ here is called taking *normal closure*. It comes from trying to force the image invariance property in the characterisation of finite normal extensions.

7 Finite fields, Frobenius lifts and existence of non-solvable quintic

By the characterisation of solvability over characteristic zero, to show that there exists quintics with roots *inexpressible* in terms of basic arithmetic and radicals, it suffices to give an irreducible quintic with non-solvable Galois group. We claim that $T^5 - T - 1 \in \mathbb{Q}[T]$ has Galois group S_5 which is not solvable. To compute its Galois group, we introduce an effective technique using *finite fields* called *Frobenius lifts*.

> **Definition**
> Let A be a ring where $p = 0$. The *Frobenius map* is the map $x \mapsto x^p$ on A. This is a ring morphism by freshman's dream.

> **Proposition – Classification of finite fields**
> Let $p > 0$ be a prime.
>
> - (Existence) For $n > 0$, let $\mathbb{F}_{p^n}$ be a splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$. Then $\mathbb{F}_{p^n}$ is a field with p^n elements. This is well-defined up to isomorphism as $\mathbb{F}_p$ extensions.
> - (Uniqueness) Any finite extension $\mathbb{F}_p \to F$ must be isomorphic to $\mathbb{F}_{p^n}$ for some $n > 0$ as extensions of $\mathbb{F}_p$.
> - (Galois) $\mathbb{F}_p \to \mathbb{F}_{p^n}$ is finite Galois with Galois group cyclic order n generated by the Frobenius map $x \mapsto x^p$.
>
>   More generally, for $0 < n$ and $0 \leq d$, the extension $\mathbb{F}_{p^n} \to \mathbb{F}_{p^{n+d}}$ is finite Galois with Galois group cyclic order d generated by $x \mapsto x^{p^n}$.

Proof. (Existence) Because the Frobenius is a ring morphism on $\mathbb{F}_{p^n}$, the set of roots of $X^{p^n} - X$ forms a subfield containing $\mathbb{F}_p$. It follows that this must be all of $\mathbb{F}_{p^n}$.

(Uniqueness) Let $n := [F : \mathbb{F}_p]$. Then $|F| = p^{[F:\mathbb{F}_p]}$. By Lagrange's theorem on groups, we have that any $x \in F^\times$ must satisfy $x^{|\mathbb{F}_p^\times|} - 1 = 0$. It follows that the elements of F are precisely all the roots of the polynomial $X^{p^n} - X$ and hence must be a splitting field for it.

(Galois) For $x \in \mathbb{F}_{p^n}$, $x^p = x$ iff $x \in \mathbb{F}_p$. The result follows from the characterisation of finite Galois extensions. We leave the general case as an exercise. $\square$

> *Example.*
> *Let us find all the monic irreducible quadratics in $\mathbb{F}_3[T]$. By the classification of finite fields, they are precisely the minimal polynomials of $x \in \mathbb{F}_9 \setminus \mathbb{F}_3$. This implies there are precisely three of them. At this point we can guess. The following quadratics do not have roots in $\mathbb{F}_3$ and hence are irreducible.*
>
> - $T^2 + 1$
> - $T^2 - T - 1$
> - $T^2 + T - 1$

> **Proposition – Frobenius lifts**
> Let $f \in \mathbb{Z}[T]$ be monic and separable, $\mathbb{Q} \to K$ a splitting field of f. Let $S \subseteq K$ be the set of roots of f and consider the subring generated by S
>
> $$A := \mathbb{Z}[S] \subseteq K$$
>
> Let $p > 0$ be a prime such that the mod p reduction $\overline{f} \in \mathbb{F}_p[T]$ is separable. Then :
>
> 1. There exists a maximal ideal $\mathfrak{q} \subseteq A$ which contains p. We call $\mathfrak{q}$ a *prime lying above p*.
> 2. Let $\mathfrak{q}$ be a prime lying above p. Define the *decomposition group*
>
> $$D(\mathfrak{q}/p) := \{\sigma \in \operatorname{Gal}(K/\mathbb{Q}) \text{ s.t. } \sigma(\mathfrak{q}) = \mathfrak{q}\}$$
>
>   Then
>
>   (a) $\kappa(\mathfrak{q}) := A/\mathfrak{q}$ is a splitting field of $\overline{f}$
>
>   (b) The ring morphism $\mathbb{Z}[S] \to \kappa(\mathfrak{q}), x \mapsto \overline{x}$ induces a bijection between S and its image $\overline{S}$. The action of $D(\mathfrak{q}/p)$ on S is compatible with the action of $\operatorname{Gal}(\kappa(\mathfrak{q})/p)$ on $\overline{S}$, i.e. the following diagram commutes
>
> $$\begin{tikzcd} D(\mathfrak{q}/p) \times S \arrow[r] \arrow[d] & S \arrow[d, "\sim"] \\ \operatorname{Gal}(\kappa(\mathfrak{q})/p) \times \overline{S} \arrow[r] & \overline{S} \end{tikzcd}$$
>
>   (c) The group morphism $D(\mathfrak{q}/p) \to \operatorname{Gal}(\kappa(\mathfrak{q})/\mathbb{F}_p)$ is bijection.
>
>   In particular, there exists a unique $\phi \in \operatorname{Gal}(K/\mathbb{Q})$ which such that $\phi|_A = \operatorname{Frob} \bmod \mathfrak{q}$.

Let's see the applications to Galois groups before the proof.

> **Proposition – Dedekind's result on cycle shapes**
> Let $f \in \mathbb{Z}[T]$ be monic separable, $K/\mathbb{Q}$ a splitting field and $S \subseteq K$ the set of its roots. Let $p > 0$ a prime such that mod p reduction $\overline{f} \in \mathbb{F}_p[T]$ is separable. Suppose that $\overline{f}$ factors into irreducible polynomials of degree $n_1, \ldots, n_r$. Then there exists $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ such that under the injection $\operatorname{Gal}(K/\mathbb{Q}) \to \operatorname{Aut} S$, σ has cycle shape $(n_1) \cdots (n_r)$.

Proof. Let $\mathfrak{q}$ be as in the previous proposition and σ be a Frobenius lift from $\kappa(\mathfrak{q})$. Then the cycle shape of σ acting on S is the cycle shape of the Frobenius acting on $\overline{S}$. The cycles are precisely the orbits under the action of the Galois group $\operatorname{Gal}(\kappa(\mathfrak{q})/p)$. Elements of each orbit share the same minimal polynomial, and the set of minimal polynomials ranging across the orbits is precisely the irreducible factors of $\overline{f}$ (up to scaling by $\mathbb{F}_p^\times$). □

> **Proposition**
> The polynomial $T^5 - T - 1 \in \mathbb{Q}[T]$ has Galois group S_5 and hence is not solvable by radicals.

Proof. Mod 2 we get $(T^2 + T + 1)(T^3 + T^2 + 1)$ which are irreducible because they do not have roots in $\mathbb{F}_2$. So there exists an element of the Galois group with cycle shape $(2)(3)$ and hence there exists one with cycle shape (2), i.e. a transposition.

Mod 3 it is irreducible. It has no roots and we can check it is not divisible by the three monic irreducible quadratics in $\mathbb{F}_3[T]$.

- $T^5 - T - 1 = (T^2 + 1)(T^3 - T) - 1$
- $T^5 - T - 1 = (T^2 - T - 1)(T^3 + T^2 - T - 1) + 1$
- $T^5 - T - 1 = (T^2 + T - 1)(T^3 - T^2 - T) + (T - 1)$

So there exists an element of the Galois group with cycle shape (5).

> *Lemma. Let $G \subseteq S_p$ where $p > 0$ is prime. Suppose G contains a tranposition and a p-cycle. Then $G = S_p$.*
>
> *Proof.* Exercise in group theory. ■

So the Galois group is S_5. The fact that this is not solvable is a group theory fact so we omit it. □

We give another application of Frobenius lifts.

> **Proposition – Cyclotomic extensions in characteristic zero**
> Let $n > 0$ and let $\mathbb{Q}(\mu_n)/\mathbb{Q}$ be a splitting field of $T^n - 1$. Recall we have a canonical isomorphism $\mathrm{Aut}_{\mathrm{Grp}}\, \mu_n \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ and hence an injection
>
> $$\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$$
>
> This is in fact an isomorphism.

Proof. Let $m \in (\mathbb{Z}/n\mathbb{Z})^\times$. This corresponds to $x \mapsto x^m \in \mathrm{Aut}_{\mathrm{Grp}}\, \mu_n$. To show m is in the image of $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$, it suffices to do case of $m = p$ a prime. By assumption, $n \not\equiv 0 \bmod p$ so $T^n - 1$ is separable over $\mathbb{F}_p$. Then we have a commuting diagram of group morphisms :

$$\begin{tikzcd}
D(\mathfrak{q}/p) \arrow[r] \arrow[d, "\simeq"] & \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \arrow[r] & \mathrm{Aut}_{\mathrm{Grp}}\mu_n(\mathbb{Q}) \arrow[d, "\simeq"'] \\
\mathrm{Gal}(\mathbb{F}_p(\mu_n)/\mathbb{F}_p) \arrow[rr] & & \mathrm{Aut}_{\mathrm{Grp}}\mu_n(\mathbb{F}_p)
\end{tikzcd}$$

This implies there's $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ which gives $x \mapsto x^p$ in $\mathrm{Aut}_{\mathrm{Grp}}\, \mu_n$. □

We can apply this to lines and circle constructions to determine which regular n-gons are constructible using lines and circles.

Definition

Let K be a field and $x, y \in L/K$ some extension. We say (x, y) is *constructible in one step from K* when it they can be obtained as solutions to the following three kinds of simultaneous equations.

1. (Line-Line intersection) $a_1x + b_1y + c_1 = 0$ and $a_2x + b_2y + c_2 = 0$.
2. (Line-circle intersection) $ax + by + c = 0$ and $x^2 + y^2 + Ax + By + C = 0$.
3. (Circle-circle intersection) $x^2 + y^2 + Ax + By + C = 0$ and $x^2 + y^2 + Rx + Sy + T = 0$

We say (x, y) is constructible from K when there exists a sequence $(x_0, y_0), \dots, (x_n, y_n)$ with $x_0, y_0 \in K$ and $x_n = x, y_n = y$ such that (x_{i+1}, y_{i+1}) is constructible from K_i in one step and $K_{i+1} := K_i(x_{i+1}, y_{i+1})$.

Proposition

Let K be a field and $x, y \in L/K$ some extension. Then (x, y) is constructible in one step from K iff $[K(x, y) : K] \leq 2$. Hence (x, y) is constructible from K iff $[K(x, y) : K]$ is a power of 2.

Proof. The three kinds of simultaneous equations are all equivalent to solving at most a quadratic equation. □

Example (Constructing regular pentagon).
We ask if we can construct the regular pentagon from $\mathbb{Q}$. This is equivalent to $(\cos(2\pi/5), \sin(2\pi/5))$ being constructible from $\mathbb{Q}$, which is equivalent to $[\mathbb{Q}(\cos(2\pi/5), \sin(2\pi/5)) : \mathbb{Q}] = 2^n$. By chucking in i, this is equivalent to $[\mathbb{Q}(\cos(2\pi/5), \sin(2\pi/5), i) : \mathbb{Q}] = 2^{n+1}$. Now $\mathbb{Q}(\mu_5) \subseteq \mathbb{Q}(\cos(2\pi/5), \sin(2\pi/5), i)$. If you chuck i into $\mathbb{Q}(\mu_5)$ then you can make $\sin(2\pi/5)$ because $\zeta := e^{2\pi i/5} = \cos(2\pi/5) + i\sin(2\pi/5)$. So the condition is equivalent to $[\mathbb{Q}(\mu_5) : \mathbb{Q}] = 2^n$. By the theory of cyclotomic extensions over $\mathbb{Q}$, $[\mathbb{Q}(\mu_5) : \mathbb{Q}] = \phi(5) = 4$ so the regular pentagon is constructible. In fact we can derive a contruction by writing $\mathbb{Q} \to \mathbb{Q}(\mu_5)$ as a tower of degree 2 extensions solving quadratics we can construct. In this case, we are lucky because $\cos(2\pi/5) = (\zeta + \zeta^{-1})/2$ which is fixed by the unique order two element in $\mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$. Indeed,

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = \zeta - \zeta^{-1} + 1$$

so

$$\cos(2\pi/5) = \frac{-1 + \sqrt{5}}{4}$$

Proposition – Characterization of constructible regular polygons
TODO

Proof of Frobenius lifts. Just as $K^G = \mathbb{Q}$, we prove $A^G = \mathbb{Z}$. The following is an "integral version" of the characterisation of finite simple extensions.

> *Lemma (Characterisation of integral elements). Let $K/\mathbb{Q}$ be an extension and $\alpha \in K$. Then α is the root of a* monic *$f \in \mathbb{Z}[X]$ iff $\mathbb{Z}[\alpha]$ is finitely generated as a $\mathbb{Z}$-module. If any of the above are satisfied, we say α is* integral over $\mathbb{Z}$*.*
>
> *Consequently, if $\alpha, \beta \in K$ are integral over $\mathbb{Z}$, then so is any $x \in \mathbb{Z}[\alpha, \beta]$.*

> *Proof.* ($\Rightarrow$) Same strategy as for algebraic elements. ($\Leftarrow$) Since $\mathbb{Z}[\alpha] \subseteq K$ which does not have any torsion, it follows from Smith normal form that $\mathbb{Z}[\alpha]$ has a $\mathbb{Z}$-basis $x_1, \ldots, x_d$. We can write $x_i = g_i(\alpha)$ for some $g_i \neq 0 \in \mathbb{Z}[X]$. Let $n =$ maximum of the degrees of g_i. Then $\alpha^{n+1} = \lambda_1 x_1 + \cdots + \lambda_d x_d$ for some $\lambda_i \in \mathbb{Z}$. Expanding out $x_i = g_i(\alpha)$ implies α satisfies $X^{n+1} - \lambda_1 g_i(X) - \cdots - \lambda_d g_d(X)$, which is monic and in $\mathbb{Z}[X]$.
>
> For the consequence, α, β integral implies $\mathbb{Z}[\alpha, \beta]$ is finitely generated as a $\mathbb{Z}$-module. This implies the submodule $\mathbb{Z}[x] \subseteq \mathbb{Z}[\alpha, \beta]$ is also, and hence x is integral over $\mathbb{Z}$. ■

The lemma implies that every element in A is integral over $\mathbb{Z}$. Then for any $x \in A^G = A \cap K^G = A \cap \mathbb{Q}$, we can write $x = a/b$ for $a, b \in \mathbb{Z}$ coprime and $b \neq 0$, and $x^d + \lambda_1 x^{d-1} + \cdots + \lambda_d = 0$ for some $\lambda_i \in \mathbb{Z}$ and $d > 0$. Then $a^d + \lambda_1 b a^{d-1} + \cdots + \lambda_d b^d = 0$ so b divides a and hence $b = \pm 1$. Thus $A^G = \mathbb{Z}$.

(1) It is a consequence of Zorn's lemma that if $p \in A$ is not a unit, then such $\mathfrak{q}$ exists. We have $1/p \notin A$ because if it were then $1/p \in A^G = \mathbb{Z}$.

(2) (a) It is a field because $\mathfrak{q}$ is maximal and it is the splitting field of $\overline{f}$ because it is generated by the image of S, which gives all the roots of $\overline{f}$. Note that $\mathfrak{q} \cap \mathbb{Z}$ is a proper ideal containing (p) so $\mathfrak{q} \cap \mathbb{Z} = (p)$.

(b) Write $f(T) = \prod_{a \in S}(T - a) \in \mathbb{Z}[S][T]$. Then $\overline{f}(T) = \prod_{a \in S}(T - \overline{a}) \in \kappa(\mathfrak{q})[T]$ where $\overline{a} = a \bmod \mathfrak{q}$. By assumption of $\overline{f}$ being separable, $a \neq b$ in S implies $\overline{a} \neq \overline{b}$. So $S \to \overline{S}$ is an injection of finite sets and hence a bijection. The compatibility of actions is clear.

(c) Injectivity follows from $S \to \overline{S}$ being bijective. Surjectivity is more subtle, we closely follow the argument from [Stacks, Lemma 0BRJ].

> *Lemma. For primes $\mathfrak{q}, \mathfrak{q}_1 \subseteq A$ lying above p, there exists $\sigma \in G := \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}_1$. It follows that there are finitely many primes lying above p.*
>
> *Proof.* Suppose for a contradiction that there exists $x \in \mathfrak{q}_1$ and not in $\sigma(\mathfrak{q})$ for any $\sigma \in G$. Then $\prod_{\sigma \in G} \sigma(x) \in \bigcap_{\sigma \in G} \sigma(\mathfrak{q}_1)$. The latter is a proper ideal of $A^G = \mathbb{Z}$ containing (p) so must be equal to (p). But then we have $\prod_{\sigma \in G} \sigma(x) \in (p) \subseteq \mathfrak{q}$ and hence $x \in \sigma^{-1}(\mathfrak{q})$ for some $\sigma \in G$, a contradiction. ■

By the Chinese remainder theorem, we have a surjection

$$A \to \prod_{\mathfrak{q}_1 \in \mathrm{Orb}(\mathfrak{q})} A/\mathfrak{q}_1$$

We know $\kappa(\mathfrak{q})$ is a finite extension of $\mathbb{F}_p$. So by the theory of finite fields and cyclotomic extensions, there exists $\overline{a}$ generating $\kappa(\mathfrak{q})^\times$. Choose $a \in A$ such that $a = \overline{a} \bmod \mathfrak{q}$ and $0 \bmod \mathfrak{q}_1 \neq \mathfrak{q}$. Now we use the Galois theory trick : $\min(a, \mathbb{Q})(T) = \prod_{\alpha \in \mathrm{Orb}(a)}(T - \alpha) \in K[T]$. Since $a \in A$ it follows that $\min(a, \mathbb{Q}) \in A[T]$. Reducing $\mathfrak{q}$, we find that the minimal polynomial of $\overline{a}$ must divide $\prod_{\alpha \in \mathrm{Orb}(a)}(T - \overline{\alpha})$. This implies $\mathrm{Frob}(\overline{a}) = \overline{\sigma(a)}$ for some $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. It STS $\sigma \in D(\mathfrak{q}/p)$. Let $x \in \mathfrak{q}$. Then $ax = 0 \bmod \bigcap_{\mathfrak{q}_1 \in \mathrm{Orb}(\mathfrak{q})} \mathfrak{q}_1$ so $\sigma(ax) = 0 \bmod \bigcap_{\mathfrak{q}_1 \in \mathrm{Orb}(\mathfrak{q})} \mathfrak{q}_1$. Looking at the $A/\mathfrak{q}$ component, $0 = \sigma(x)\sigma(a) = \sigma(x)\overline{a}^p \bmod \mathfrak{q}$ which implies $\sigma(x) = 0 \bmod \mathfrak{q}$. □

8 Bonus : Sneak peak at p-adic and perfectoid fields

To be fleshed out :

1. $\mathbb{F}_p[T]$

2. $\mathbb{F}_p[[T]] := \varprojlim_{n\geq 0} \mathbb{F}_p[T]/(T^{n+1})$. As a set we have

$$\prod_{n\geq 0} \mathbb{F}_p \xrightarrow{\sim} \mathbb{F}_p[[T]]$$

by $(a_n) \mapsto (\sum_{0\leq d\leq n} a_d T^d \bmod T^{n+1})_n$. One can check that the coefficients of sums and products are as one would expect for power series. We have an induced ring morphism

$$\mathbb{F}_p[T] \to \mathbb{F}_p[[T]]$$

It is injective because if one has a polynomial $f \in \mathbb{F}_p[T]$ which is divisible by T^{n+1} for all $n \geq 0$ then $f = 0$. Notice in the T-adic completion, $1 - T$ has an inverse given by $\sum_{d\geq 0} T^d$. Indeed, mod T^{n+1} we have

$$(1 - T)(1 + T + \cdots + T^n) = 1$$

In fact, (T) is the unique maximal ideal of $\mathbb{F}_p[[T]]$. (Hint : One idea is to use geometric series.) The geometric intuition is that $\mathbb{F}_p[T]$ is the ring of functions on the affine line, $\mathbb{F}_p[T]/(T)$ is the ring of functions at the point $\{0\}$ in the affine line. $\mathbb{F}_p[T]/(T^2)$ is the ring of functions on a subspace of the affine line that's a tiny bit bigger than just $\{0\}$. It's not bigger to the point that T can take on any values other than 0 because $T^2 = 0$. But this space is large enough to know about the first derivative of functions at $\{0\}$. This is call the *first order infinitesimal neighbourhood of* $\{0\}$. Similarly for $\mathbb{F}_p[T]/(T^{n+1})$. Finally, $\mathbb{F}_p[[T]]$ is the ring of functions on the union of these infinitesimal neighbourhoods. The fact that anything outside (T) is invertible says anything that is non-zero at zero is invertible. In this sense, we still don't have points other than zero.

One can show $\mathbb{F}_p[[T]]$ is a domain. Let $f, g \in \mathbb{F}_p[[T]]$ with $fg = 0$. Then $f_0 g_0 = 0$ so WLOG $f_1 \in \mathbb{F}_p^\times$ and $g_0 = 0$. Then $f_0 g_1 + f_1 g_0 = 0$ implies $g_1 = 0$. By induction, $g_n = 0$ for all $n \geq 0$ so $g = 0$. This means we can take fraction field

$$\mathbb{F}_p((T)) := \operatorname{Frac} \mathbb{F}_p[[T]] \simeq \mathbb{F}_p[[T]][1/T]$$

which intuitively is the ring of functions on the *punctured disk around zero*.

3. $\mathbb{Z}$ is similar to $\mathbb{F}_p[T]$ in the sense that elements can be written uniquely as polynomials with coefficients in $\{0, \ldots, p-1\}$. In $\mathbb{Z}$ the "variable" is p and unlike $\mathbb{F}_p$, there's a non-trivial "carrying over" of coefficients when adding elements. For example in $\mathbb{Z}$

$$(0 \cdot 1 + 3 \cdot 5) + (0 \cdot 1 + 2 \cdot 5) = (0 \cdot 1 + 0 \cdot 5 + 1 \cdot 5^2)$$

whilst in $\mathbb{F}_5[T]$

$$(0 + 3T) + (0 + 2T) = 0$$

An idea is that we can play the same game of completion with p instead of T. The resulting ring is called the *p-adic integers*.

$$\mathbb{Z}_p := \varprojlim_{n\geq 0} \mathbb{Z}/(p^{n+1})$$

By the same argument as for $\mathbb{F}_p[T]$ we have an injection

$$\mathbb{Z} \to \mathbb{Z}_p$$

Again, as sets we have

$$\prod_{n \geq 0} \{0, \cdots, p-1\} \xrightarrow{\sim} \mathbb{Z}_p$$
$$(a_n)_n \mapsto (\sum_{0 \leq d \leq n} a_d p^d \bmod p^{n+1})_n$$

This is not too useful because of the non-trivial "carrying over" of coefficients when adding and multiplying unlike the case of $\mathbb{F}_p[[T]]$.

One can also show $\mathbb{Z}_p$ has (p) as the unique maximal ideal. The key is that in$\mathbb{Z}/(p^{n+1})$, p is nilpotent so any maximal ideal must contain (p), which is maximal itself. It follows that (p) is the unique maximal ideal of $\mathbb{Z}/(p^{n+1})$ for all $n \geq 0$. So if $x \in \mathbb{Z}_p$ with $x \neq 0 \bmod p$, then $x \bmod p^{n+1}$ is invertible for all $n \geq 0$ and hence x is invertible. [1]

Geometrically, if one pretends $\mathbb{Z}$ is the ring of functions on some space and p is a point in that space, then one can imagine $\mathbb{F}_p = \mathbb{Z}/(p)$ as the ring of functions at the point p and $\mathbb{Z}_p$ as the ring of functions on the formal disk around p.

One can also show $\mathbb{Z}_p$ is a domain. The key is p-torsion-free.

> *Lemma. For $x \in \mathbb{Z}_p$, if $px = 0$ then $x = 0$.*
>
> *Proof.* Write $x = \sum_{n \geq 0} x_n p^n$ with $x_n \in \{0, \cdots, p-1\} \subseteq \mathbb{Z}$. Mod p^2 we have $px_0 = 0$ so $x_0 = 0$. Mod p^3 we have $0 = p(x_1 p + x_2 p^2) = x_1 p^2$ so $x_1 = 0$. By induction $x_n = 0$ for all n. ■

Let $x, y \in \mathbb{Z}_p$ with $xy = 0$. Writing both as p-adic expansions with coefficients in $[0, p-1] \cap \mathbb{Z}$ gives $x_0 y_0 = 0 \bmod p$ and hence $x_0 = 0$ or $y_0 = 0$. WLOG $x_0 \in \mathbb{F}_p^\times$ and $y_0 = 0$. Then we can write $0 = xy = px(y_1 + y_2 p + \cdots)$ and so $x(y_1 + y_2 p + \cdots) = 0$ in $\mathbb{Z}_p$. By induction, $y_n = 0$ for all n and hence $y = 0$.

Thus, we can take fraction fields and obtain the *p-adic rationals*.

$$\mathbb{Q}_p := \operatorname{Frac} \mathbb{Z}_p \simeq \mathbb{Z}_p[1/p]$$

Intuitively, this is the ring of functions on the punctured disk around p.

4. Why is this useful? Recall in the section on cyclotomic extensions, we proved that $\mathbb{F}_p^\times$ is cyclic effectively by counting. Let us give a different proof by relating $\mathbb{F}_p^\times$ with $(p-1)$-th roots of unity in $\mathbb{C}$, which we know is cyclic because it is generated by $e^{2\pi i/(p-1)}$.

   Recall we wrote elements of $\mathbb{Z}_p$ as power series in p with coefficients by picking $\{0, \ldots, p-1\} \subseteq \mathbb{Z} \subseteq \mathbb{Z}_p$ as lifts of $\mathbb{F}_p^\times$ under $\mathbb{Z}_p \to \mathbb{F}_p$. This does not reflect the additive nor multiplicative nature of elements in $\mathbb{F}_p^\times$. We cannot expect addition of lifts to be respected because $p = 0$ in $\mathbb{F}_p$ but $p \neq 0$ in $\mathbb{Z} \subseteq \mathbb{Z}_p$. We now show that there is a better choice of coefficients which is multiplicative. More precisely,

---

[1] This strategy also works for $\mathbb{F}_p[[T]]$.

> *Lemma. There exists a unique multiplicative map* $[\_] : \mathbb{F}_p \to \mathbb{Z}_p$ *such that* $[x] = x \bmod p$.
>
> *Proof.* The idea is that for $x = y \in \mathbb{F}_p = \mathbb{Z}/(p)$, although we cannot in general lift x, y so that $x = y \bmod p^2$ we do have $x^p = y^p \bmod p^2$ by binomial expansion. Take $x \in \mathbb{F}_p$, we define $[x] \bmod p^{n+1}$ for each $n \geq 0$:
>
> (a) Take $x^{1/p} \in \mathbb{F}_p$, which is unique by the Frobenius being bijective.
>
> In general, take x^{1/p^n}.
>
> (b) Take *any* lift $x_1 \in \mathbb{Z}/(p^2)$ of $x^{1/p}$.
>
> For general n take any lift $x_n \in \mathbb{Z}/(p^{n+1})$ of x^{1/p^n}.
>
> (c) Take $[x]_1 := x_1^p \in \mathbb{Z}/(p^2)$. This only depends on the value of $[x]_1 \bmod p$ which is $[x]_1 = x_1^p = (x^{1/p})^p = x \bmod p$.
>
> For any n, take $[x]_n := x_n^{p^n} \in \mathbb{Z}/(p^n)$. This depends only on the value of $[x]_n \bmod p$ which is again x.
>
> (d) Because $(x^{1/p^{n+1}})^p = x^{1/p^n} \bmod p$ we have $[x]_{n+1} = (x_{n+1}^p)^{p^n} = x_n^{p^n} = [x]_n \bmod p^n$. This defines $[x] \in \mathbb{Z}_p$.
>
> For $x, y \in \mathbb{F}_p$, $x_n y_n$ lifts $(xy)^{1/p^n}$ so $[x]_n[y]_n = x_n^{p^n} y_n^{p^n} = [xy]_n \bmod p^{n+1}$. It follows that $[x][y] = [xy]$. Uniqueness is straightforward to check. ■

In particular, $[\mathbb{F}_p^\times] \subseteq \mathbb{Z}_p$ gives $(p-1)$-th roots of unity! Furthermore, mod p gives a group isomorphism $[\mathbb{F}_p^\times] \simeq \mathbb{F}_p^\times$. So we have lifting the $(p-1)$-th roots of unity in characteristic p to characteristic zero.

Now note $\mathbb{Z} \subseteq \mathbb{Z}_p$ induces a field extension $\mathbb{Q} \to \mathbb{Q}_p$ (of infinite degree). Take $\mathbb{Q}([\mathbb{F}_p^\times])$ which is a finite subextension. This must be a splitting field for $X^{p-1} - 1 \in \mathbb{Q}[X]$. By the embedding theorem, we must have some isomorphism $\mathbb{Q}([\mathbb{F}_p^\times]) \simeq \mathbb{Q}(e^{2\pi i/(p-1)})$ as extensions of $\mathbb{Q}$ since both are splitting fields of $X^{p-1} - 1$. Under this unknown isomorphism, $[\mathbb{F}_p^\times] \simeq \langle e^{2\pi i/(p-1)} \rangle$. Thus we conclude $\mathbb{F}_p^\times$ is cyclic.

5. Define $\mathbb{F}_p((t^{1/p^\infty}))$ and $\mathbb{Q}_p^\infty$. State Fontaine–Winterberger isomorphism. [FW83]

   These are examples of *perfectoid fields*. Just as fields generalise to rings, perfectoid fields generalise to *perfectoid rings*. The applications of these rings falls in the area called *p-adic Hodge theory*. Describing this is beyond the scope of these talks. Let's just say they were significant enough to win Peter Scholze the Fields medal in 2018!

6. (If time permits) Tilting $\mathbb{Q}_p^\infty$ to $\mathbb{F}_p((t^{1/p^\infty}))$.

References

[FW83] J.-M. Fontaine and J.-P. Wintenberger. "Le corps des normes de certaines extensions infinies de corps locaux ; applications". fr. In: *Annales scientifiques de l'École Normale Supérieure* 4e série, 16.1 (1983), pp. 59–89. URL: `http://www.numdam.org/articles/10.24033/asens.1440/`.

[Stacks] T. Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`. 2018.