

1. Each  $F$ -Automorphism of  $K$  is an extension of the embedding  $F \rightarrow F^{\text{alg}}$  which is identity on  $F$  to  $K$ , and hence  $n = \#G \leq [K : F]_{\text{sep}} \leq [K : F]$ . To prove the opposite inequality, consider  $\alpha_1, \dots, \alpha_m \in K$  such that  $m > n$ . Then the system of equations

$$\begin{aligned} a_1\tau_1(\alpha_1) + a_2\tau_1(\alpha_2) + \dots + a_m\tau_1(\alpha_m) &= 0 \\ \vdots \\ a_1\tau_n(\alpha_1) + a_2\tau_n(\alpha_2) + \dots + a_m\tau_n(\alpha_m) &= 0 \end{aligned}$$

With  $n$  equations, and  $m$  unknowns. Then the equation must have a (non-zero) solution, we wish to show that it has a solution lying in  $F$ , which would prove that we cannot have more than  $n$   $F$ -linearly independent elements of  $K$ . Suppose that  $(b_1, \dots, b_m)$  is a solution with the most non-zero terms, WLOG we can take  $b_1 \neq 0$ , and further take  $b_1 = 1$  by dividing the each  $b_i$  by  $b_1$ . Then for each  $\tau_i$ , since  $\tau_i(0) = 0$ , and  $\tau_i$  permutes the other  $\tau_j$  since  $G$  is a group, we get that applying any  $\tau_i$  to the system of equations yields another solution, with the same zero terms. But then  $(1 - \tau_i(1), \dots, b_m - \tau_i(b_m))$  is another solution, with the same zero coordinates as  $b$ , along with the first coordinate being 0 which by our minimality assumption implies that this is the zero vector. Since this holds for each  $\tau_i$ , it follows that  $\tau_i(b_j) = b_j$  for each  $i, j$ , so that each  $b_j$  is fixed by  $G$  and thus lies in  $F$ , hence the first equation gives us that  $\alpha_1, \dots, \alpha_m$  are  $F$ -linearly dependent, so no  $F$ -linearly independent set of  $K$  may have cardinality greater than  $n$ , i.e.  $[K : F] \leq n$ . Since we have proven both inequalities,  $[K : F] = n$ .

2. Since  $K/F$  is finite, we may write it as  $K = F(\alpha_1, \dots, \alpha_n)$ . It is immediate that since  $\{\alpha_1, \dots, \alpha_n\} \subset K \subset KL$ , that we can write  $KL = L(\alpha_1, \dots, \alpha_n)$ , since this field contains  $F$  and each  $\alpha_i$  it must contain  $K$ . Since each  $\alpha_i$  satisfies a polynomial with coefficients in  $F \subset L$ , we know that  $KL/L$  is algebraic. To show that its separable, note that  $\min(\alpha_i; L) \mid \min(\alpha_i; F)$ , where  $\min(\alpha_i; F)$  contains no repeated roots, proving that each  $\alpha_i$  is separable over  $L$ . Finally, since  $K/F$  is normal of finite degree, we know that  $K$  is the splitting field of some polynomial  $f \in F[x]$ , it is immediate that  $L(\alpha_1, \dots, \alpha_n)$  is the splitting field of  $f$  over  $L$ , so that  $KL/L$  is normal and hence Galois.

Consider the map  $\pi : \text{Gal}(KL/L) \rightarrow \text{Gal}(K/(K \cap L))$ , defined by  $\sigma \mapsto \sigma|_K$ . It is clear that this map is well defined, and satisfies the homomorphism properties. To check this is an isomorphism, suppose that  $\sigma \in \ker \pi$ , then  $\sigma|_K = 1$ , hence  $\sigma(\alpha_i) = \alpha_i$  for each  $i$ , furthermore  $\sigma$  fixes  $L$  by definition. It follows that for any  $x \in KL$ , we have  $x = \sum_i \left( \ell_i \prod_j \alpha_j \right)$ , so that

$$\sigma(x) = \sigma \left( \sum_i \left( \ell_i \prod_j \alpha_j \right) \right) = \sum_i \left( \sigma(\ell_i) \prod_j \sigma(\alpha_j) \right) = x$$

implying that  $\sigma = 1$ , so that this map is injective. To show surjectivity, let  $\tau \in \text{Gal}(K/(K \cap L))$ , define  $\sigma(\alpha_i) = \tau(\alpha_i)$ , this is a well defined extension of the identity map on  $L$ , since if  $\alpha_i, \alpha_j$  are conjugate over  $K \cap L$ , then they are conjugate over  $L$ . This can be seen since

$$\min(\alpha; L) \mid \min(\alpha; K \cap L) \text{ and } \min(\alpha; L) = (x - \alpha)(x - \beta_1) \cdots (x - \beta_k)$$

for  $\beta_i \in K$ , then the coefficients of  $\min(\alpha; L)$  are the symmetric polynomials in  $\alpha, \beta_1, \dots, \beta_k$  so that they also lie in  $K$ , so that in particular the coefficients lie in  $K \cap L$ , this implies that  $\min(\alpha; L)$  is a polynomial with coefficients in  $K \cap L$  which is satisfied by  $\alpha$ , implying that

$\min(\alpha; K \cap L) | \min(\alpha; L)$ , so that in particular they are equal. Then by construction, we get  $\sigma|_K = \tau$  proving surjectivity. Since this is an isomorphism between the two Galois groups it is also a bijection, so in particular

$$[KL : L] = \#\text{Gal}(KL/L) = \#\text{Gal}(K/K \cap L) = [K : K \cap L]$$

**3.** First note that

$$\bigcap_{\sigma \in G} \sigma H \sigma^{-1} = \bigcap_{\sigma \in G} \text{Gal}(K/\sigma(L))$$

This follows since  $\tau \mapsto \sigma \tau \sigma^{-1}$  is a bijection from  $H$  to  $\text{Gal}(K/\sigma(L))$ .

We first show that  $\text{Gal}(K/N) \subset \bigcap_{\sigma \in G} \text{Gal}(K/\sigma(L))$ . Proof being, since  $N \supset L$  is normal, for any  $\sigma \in G$ , we have  $\sigma(L) \subset \sigma(N) = N$ . Thus if  $\tau|_N = 1$ , then  $\tau|_{\sigma(L)} = 1$  for any  $\sigma \in G$ . This suffices to show that  $\tau \in \text{Gal}(K/N)$  implies  $\tau \in \bigcap_{\sigma \in G} \text{Gal}(K/\sigma(L))$ .

Now we show the other inclusion, namely  $\text{Gal}(K/N) \supset \bigcap_{\sigma \in G} \text{Gal}(K/\sigma(L))$ . Since  $N$  is the compositum  $\langle \sigma(L) \rangle_{\sigma \in G}$  (proven below), we have that  $\tau \in \bigcap_{\sigma \in G} \text{Gal}(K/\sigma(L))$ , then  $\tau|_N = 1$ , since for any  $\alpha$  in  $N$ , we can write  $\alpha$  as a finite sum/product/quotient of elements in  $\bigcup_{\sigma \in G} \sigma(L)$ , each of which is fixed by  $\tau$ , so that  $\tau$  fixes  $\alpha$  by the homomorphism property. It follows that  $\tau \in \text{Gal}(K/N)$  proving that indeed  $N = \bigcap_{\sigma \in G} \text{Gal}(K/\sigma(L)) = \bigcap_{\sigma \in G} \sigma H \sigma^{-1}$ .

Proof of  $N = \langle \sigma(L) \rangle_{\sigma \in G}$ : the right to left inclusion is obvious by normality, then by definition of normal closure, it will suffice to show that  $\langle \sigma(L) \rangle_{\sigma \in G}$  is normal. Let  $\tau \in G$ , then we have that

$$\tau(\langle \sigma(L) \rangle_{\sigma \in G}) = \langle \tau \sigma(L) \rangle_{\sigma \in G} = \langle \sigma(L) \rangle_{\sigma \in G}$$

The second equality follows since  $\tau : G \rightarrow G$  bijectively. The first equality follows from if  $\alpha$  in  $\langle \sigma(L) \rangle_{\sigma \in G}$ , we can write  $\alpha$  as a finite sum/product/quotient of elements in  $\bigcup_{\sigma \in G} \sigma(L)$ , by the homomorphism property, we apply  $\tau$  to each element in the sum/product/quotient so that  $\alpha$  is a finite sum/product/quotient of elements in  $\bigcup_{\sigma \in G} \tau \sigma(L)$

**4.** Since  $K/F$  is Galois, and  $K \supset L_0 \supset F$ , we have  $K/L_0$  is Galois, with Galois group  $N(H)$ . Then since  $H$  is normal in  $N(H)$ , we have  $L/L_0$  is Galois. Furthermore, suppose that  $L \supset M \supset F$ , with  $L/M$  Galois implying that  $H$  is normal in  $\text{Gal}(K/M)$ . Then since the normalizer is the largest subgroup  $R$  of  $G$ , such that  $H \subset R$  is normal, we get that  $\text{Gal}(K/M) \subset N(H)$ , implying that  $M \supset L_0$  as desired.

**5.** We can define the map  $\varphi : \mathbb{Z}/2\mathbb{Z} \xrightarrow{\varphi} (\mathbb{Z}/4\mathbb{Z})$  as  $\varphi(1) : x \mapsto -x$ , this is a well defined automorphism, since  $\varphi(1)^2 = \mathbf{1}_{\mathbb{Z}/4\mathbb{Z}} = \varphi(0) = \varphi(1+1)$ . Any element  $x \in D_4$  can be written in the form of  $\sigma^i \tau^j$  using the relation  $\sigma \tau = \tau \sigma^{-1}$ . So define the map

$$\begin{aligned} \psi : D_4 &\rightarrow \mathbb{Z}/4\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z} \\ \sigma^i \tau^j &\mapsto (i, j) \end{aligned}$$

is an isomorphism.  $\mathbf{1} \mapsto (0, 0)$  is immediate. And (here I deal with both possible cases  $j = 1, 0$  separately)

$$\begin{aligned} \psi(\sigma^i \tau \sigma^k \tau^\ell) &= \psi(\sigma^{i-k} \tau^{1+\ell}) = (i-k, 1+\ell) = (i+\varphi(1)(k), 1+\ell) = (i, 1)(k, \ell) = \psi(\sigma^i \tau) \psi(\sigma^k \tau^\ell) \\ \psi(\sigma^i \tau^0 \sigma^k \tau^\ell) &= \psi(\sigma^{i+k} \tau^\ell) = (i+k, \ell) = (i+\varphi(0)(k), 0+\ell) = (i, 0)(k, \ell) = \psi(\sigma^i \tau^0) \psi(\sigma^k \tau^\ell) \end{aligned}$$

This proves that  $\psi$  is a homomorphism, and

$$\psi(\sigma^i \tau^j) = (0, 0) \iff i \equiv 0 \pmod{4} \text{ and } j \equiv 0 \pmod{2} \iff \sigma^i \tau^j = \mathbf{1}$$

proving that  $\ker \psi = \mathbf{1}$ . Then since  $\#D_4 = \# \mathbb{Z}/4\mathbb{Z} \rtimes_{\varphi} \mathbb{Z}/2\mathbb{Z}$  and the map is injective, it must also be surjective.