

**Exersise 5.1**

We can define

$$\alpha = \frac{1}{\text{Tr}(\theta)} \left( \beta\theta + (\beta + \beta^\sigma)\theta^\sigma + \dots \left( \sum_{i=0}^k \beta^{\sigma^i} \right) \theta^{\sigma^k} + \dots + \left( \sum_{i=0}^{n-2} \beta^{\sigma^i} \right) \theta^{\sigma^{n-2}} \right)$$

Where  $\theta \in K$  is chosen so that  $\text{Tr}(\theta) \neq 0$  (this can always be done since  $\sigma, \sigma^2, \dots, \sigma^n$  are linearly independent)

We have that

$$\alpha^\sigma = \frac{1}{\text{Tr}(\theta)} \left( \beta^\sigma \theta^\sigma + (\beta^\sigma + \beta^{\sigma^2})\theta^{\sigma^2} + \dots \left( \sum_{i=0}^k \beta^{\sigma^{i+1}} \right) \theta^{\sigma^{k+1}} + \dots + \left( \sum_{i=0}^{n-2} \beta^{\sigma^{i+1}} \right) \theta^{\sigma^{n-1}} \right)$$

Notice that

$$\text{Tr}(\beta) = \sum_{i=0}^{n-1} \beta^{\sigma^i} = 0 \Rightarrow \sum_{i=0}^{n-2} \beta^{\sigma^{i+1}} = -\beta$$

Pairing up terms we have the following cancelation

$$\begin{aligned} \alpha - \alpha^\sigma &= \frac{1}{\text{Tr}(\theta)} \left( \beta\theta + (\beta + \beta^\sigma - \beta^\sigma)\theta^\sigma + \dots \left( \beta + \sum_{i=1}^k \beta^{\sigma^i} - \beta^{\sigma^i} \right) \theta^{\sigma^k} + \dots + \beta\theta^{\sigma^{n-1}} \right) \\ &= \beta \frac{\text{Tr}(\theta)}{\text{Tr}(\theta)} = \beta \end{aligned}$$

Thus we have

$$\alpha - \alpha^\sigma = \beta$$

**Exersise 5.2**

Since  $K/k$  is Galois, we know that  $K$  is Galois over the intermediate field  $k' = K \cap \ell \supseteq k$  as well since it is still the splitting field of the same seperable polynomial  $f$  over  $k$ . Letting  $\alpha_1, \alpha_2, \dots, \alpha_n \notin K \cap \ell$  be the roots of  $f$  not in  $k'$  we have that

$$K = k'(\alpha_1, \alpha_2, \dots, \alpha_n)$$

When considering the extension  $K\ell/\ell$  we have that

$$K\ell = \ell(\alpha_1, \alpha_2, \dots, \alpha_n)$$

Since  $K = k'(\alpha_1, \dots, \alpha_n) \subseteq \ell(\alpha_1, \dots, \alpha_n)$  and  $\ell \subseteq \ell(\alpha_1, \dots, \alpha_n)$  which leads to  $K\ell \subseteq \ell(\alpha_1, \dots, \alpha_n)$  while conversly  $\ell(\alpha_1, \dots, \alpha_n) \subseteq K\ell$  since  $\alpha_1, \dots, \alpha_n \in K$

Thus  $K\ell$  is the splitting field of  $f$  over  $\ell$  and thus Galois

We have the isomorphism

$$\Phi : \text{Gal}(K\ell/\ell) \rightarrow \text{Gal}(K/k')$$

$$\varphi \rightarrow \varphi|_K$$

$\Phi$  is injective since every automorphism in both  $\text{Gal}(K\ell/\ell)$  and  $\text{Gal}(K/k')$  is fully determined by the image of  $\alpha_1 \dots \alpha_n$  so if  $\varphi|_K = \psi|_K$  then they must act the same way on  $\alpha_1 \dots \alpha_n$  and thus must be the same automorphisms to begin with

$\Phi$  is surjective as follows:

We have that  $H = \text{im}(\Phi)$  is a subgroup of  $\text{Gal}(K/k')$ . If we show that the fixed field of  $H$  is precisely  $k'$  then from the correspondence of Galois theory it must be the case  $\text{im}(\Phi) = \text{Gal}(K/k')$

We have that for any  $\alpha \in K \setminus k'$ , we have that  $\alpha \notin \ell$  and thus there is an isomorphism

$$\varphi : \ell(\alpha) \rightarrow \ell(\beta)$$

$$\alpha \rightarrow \beta$$

where  $\beta \neq \alpha$  is another root of the minimal polynomial of  $\alpha$  over  $\ell$ . Since  $K\ell$  is a splitting field this isomorphism extends to an automorphism

$$\psi : K\ell/\ell$$

Thus we have  $\psi|_K \in H$  is an automorphism which does not fix  $\alpha$ . Thus it must be the case the fixed field is  $k'$

We have that

$$|\text{Gal}(K\ell/\ell)| = |\text{Gal}(K/K \cap \ell)|$$

so

$$[K\ell : \ell] = [K : K \cap \ell]$$

multiplying on both sides by  $[\ell : k][K \cap \ell : k]$

$$[K\ell : \ell][\ell : k][K \cap \ell : k] = [K : K \cap \ell][\ell : k][K \cap \ell : k]$$

$$[K\ell : k][K \cap \ell : k] = [K : k][\ell : k]$$

### Exercise 5.3

We have the isomorphism

$$\Phi : \text{Gal}(K_1K_2/k) \rightarrow \text{Gal}(K_1/k) \times \text{Gal}(K_2/k)$$

$$\varphi \rightarrow (\varphi|_{K_1}, \varphi|_{K_2})$$

$\Phi$  is injective as follows. Since,  $K_1, K_2, K_1K_2$  are splitting fields,

$$K_1 = k(\alpha_1 \dots \alpha_n), K_2 = k(\beta_1 \dots \beta_m)$$

$$K_1K_2 = k(\alpha_1 \dots \alpha_n, \beta_1, \dots, \beta_m)$$

We have that  $\varphi \in \text{Gal}(K_1K_2/k)$  is completely determined by the image of  $\alpha_1 \dots \alpha_n, \beta_1 \dots \beta_m$ , yet every element in  $\text{Gal}(K_1/k)$  and  $\text{Gal}(K_2/k)$  is determined by the images of  $\alpha_1 \dots \alpha_n$  or  $\beta_1 \dots \beta_m$  respectively. Thus if  $(\varphi|_{K_1}, \varphi|_{K_2}) = (\psi|_{K_1}, \psi|_{K_2})$  then it must be the case that  $\varphi = \psi$  since they act the same way on  $\alpha_1 \dots \alpha_n, \beta_1 \dots \beta_n$

$\Phi$  is surjective as follows:

We have that  $H = \text{im}(\Phi)$  is a subgroup of  $\text{Gal}(K_1/k) \times \text{Gal}(K_2/k)$ . If we define the following groups

$$H_1 = H \cap (\text{Gal}(K_1/k) \times \{\text{id}\})$$

and

$$H_2 = H \cap (\{\text{id}\} \times \text{Gal}(K_2/k))$$

If we show

$$H_1 = \text{Gal}(K_1/k) \times \{\text{id}\}$$

$$H_2 = \{\text{id}\} \times \text{Gal}(K_2/k)$$

then we have shown

$$H = \text{Gal}(K_1/k) \times \text{Gal}(K_2/k)$$

and thus  $\Phi$  is surjective.

Under the canonical isomorphism  $H_1, H_2$  are subgroups of  $\text{Gal}(K_1/k), \text{Gal}(K_2/k)$  respectively. Thus if we show that they each have fixed field  $k$ , then we have shown that each is isomorphic to their respective Galois group and thus be able to conclude that  $\Phi$  is surjective. To show that the fixed field of  $H_1$  is  $k$ , consider any  $\alpha \in K_1 \setminus k$ . There exists the isomorphism

$$\varphi : k(\alpha) \rightarrow k(\beta)$$

$$\alpha \rightarrow \beta$$

where  $\beta \neq \alpha$  is a root of the same minimal polynomial over  $k$ . Since  $K_1K_2$  is a splitting field of  $k(\alpha)$  this isomorphism extends to an automorphism  $\psi \in \text{Gal}(K_1K_2/k)$ . We have that

$$(\psi|_{K_1}, \text{id}) \in H_1$$

And thus  $H_1$  does not fix  $\alpha$  so the fixed field of  $H_1$  must be  $k$ . The argument for  $H_2$  is the same with the appropriate relabeling

#### Exercise 5.4

We will define

$$\tilde{K} = \bigcup_{\varphi \in \text{Aut}(\bar{k}/k)} \varphi(K)$$

We have that  $\tilde{K}$  is Galois by the fact that the fixed field of  $\text{Aut}(\tilde{K}/k)$  is  $k$ . The reason for this is because for any  $\alpha \in \tilde{K} \setminus k$ , there exists an automorphism

$$\varphi : k(\alpha) \rightarrow k(\beta)$$

which extends to

$$\phi \in \text{Aut}(\bar{k}/k)$$

that sends  $\alpha$  to some other root  $\beta$  of the minimal polynomial of  $\alpha$  and thus does not fix  $\alpha$ . Thus  $\phi|_{\tilde{K}} \in \text{Aut}(\tilde{K}/k)$  is an automorphism that does not fix  $\alpha$

We have that for any Galois extension  $K'/k$  with  $K \subseteq K'$  if there exists  $\alpha \in \tilde{K} \setminus K'$ , from how  $\tilde{K}$  was constructed, there exists  $\varphi \in \text{Aut}(\bar{k}/k)$  and  $\beta \in K \setminus k$  so that  $\alpha = \varphi(\beta)$ . This would lead to a contradiction since  $\alpha$  and  $\beta$  must be roots of the same minimal polynomial  $m(x) \in k[x]$  yet  $\beta \in K'$  while  $\alpha \notin K'$  so  $m(x)$  does not split over  $K'$  which means  $K'$  is not a splitting field so not Galois.

### Exercise 5.5

We have that  $\mathbb{F}_{p^n}^*$  is a cyclic group. The reason for this is because by our classification of finite abelian groups

$$\mathbb{F}_{p^n}^* \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \dots \mathbb{Z}/n_k\mathbb{Z}$$

with  $n_1|n_2|\dots n_k$ . However if  $k > 1$  then the polynomial  $x^{n_2} - x$  would have more than  $n_2$  roots which is not possible. Thus if we let  $\theta$  be a generator of  $\mathbb{F}_{p^n}^*$  we have

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$$

We have that there exists an irreducible polynomial of degree  $n$  over  $\mathbb{F}_p$  for any  $n > 0$  we can construct the splitting field of  $x^{p^n} - x$  and use that it is a simple extension to conclude

$$\mathbb{F}_{p^n} = \mathbb{F}_p(\theta) \cong \mathbb{F}_p[x]/(m_\theta(x))$$

where  $m_\theta$  is the minimal polynomial of  $\theta$ . We have that  $m_\theta$  is the desired polynomial:

$$n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = \deg(m_\theta)$$

### Exercise 5.6

$\mathbb{Q}(\zeta_n)/\mathbb{Q}$  is Galois since it is the splitting field of the cyclotomic polynomial (which is irreducible and thus separable)

$$\Phi_n(x)$$

We know that every automorphism  $\varphi \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  is fully determined by mapping  $\zeta_n$  to another primitive root of unity. Thus the Galois group is isomorphic to the group of units in  $\mathbb{Z}/n\mathbb{Z}$

$$\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$