

**PROBLEM 1.2** (Guillot, 2018, p. 21)

Let  $F$  be a field of characteristic  $p \neq 2$ .

Let  $a \in F^\times \setminus F^{\times 2}$ , and  $K = F[\sqrt{a}]$ .

**PART 1**

Suppose there exists an extension  $L/F$  with  $K \subset L$ .

Suppose that  $L/F$  is cyclic with  $\mathbf{Gal}(L/F) \cong C_4$ .

Show that there exists an  $\alpha \in K$  such that  $N_{K/F}(\alpha) = -1$ .

*Hint:* try  $\alpha = \frac{\theta - \sigma^2(\theta)}{\sigma(\theta) - \sigma^3(\theta)}$ .

**SOLUTION 1.2.1**

Taking Guillot's hint: let  $\alpha$  be of the form  $\frac{\theta - \sigma^2(\theta)}{\sigma(\theta) - \sigma^3(\theta)}$ .

We take  $\theta$  to be an element of  $L \setminus K$ . Such a  $\theta$  must exist by dimension.

We take  $\sigma$  to be a generator of  $\mathbf{Gal}(L/F) \cong C_4$ . Let  $1_G$  be the identity.

Since  $\sigma$  fixes  $L$ ,  $\alpha$  lies in  $L$ . Since  $\sigma$  acts linearly, we have:

$$\sigma(\alpha) = \frac{\sigma(\theta) - \sigma^3(\theta)}{\sigma^2(\theta) - \theta} = -1/\alpha. \quad (1)$$

We seek  $N_{L/K}(\alpha)$ , which involves only those  $\sigma^n$  that lie in  $\mathbf{Gal}(L/K)$

To find  $\mathbf{Gal}(L/K)$  we apply *The Fundamental Theorem of Galois Theory* :

There exists normal series  $\{1_G\} \triangleleft \mathbf{Gal}(L/K) \triangleleft \mathbf{Gal}(L/F)$ .

So  $\mathbf{Gal}(L/K)$  is a normal subgroup in  $\mathbf{Gal}(L/F)$ .

The only such subgroup in  $C_4$  is given by  $\{1_G, \sigma^2\}$ .

See **Theorem 5.1** in (Morandi, 1996, p. 51) for details.

So  $N_{L/K}(\alpha) = \alpha \sigma^2(\alpha)$ , and this is equal to  $\alpha^2$  by (1) above.

Since the image of  $N_{L/K}$  is  $K$ , we now know that  $\alpha^2 \in K$ .

This implies that  $\alpha \in K$ , and we may now ask for  $N_{K/F}(\alpha)$ .

We have  $\mathbf{Gal}(K/F) \cong C_2$ . Let  $\tau$  be the non-identity which conjugates  $\sqrt{a}$ .

This automorphism is the same as the restriction of  $\sigma$  to  $K$ , denoted by  $\sigma|_K$ .

Such a compatible restriction exists by *The Isomorphism Extension Theorem*.

See **Theorem 3.20** in (Morandi, 1996, p. 34) for details.

To see that  $\tau$  is given by  $\sigma|_K$ , observe that  $\frac{\mathbf{Gal}(L/F)}{\mathbf{Gal}(L/K)} \cong \mathbf{Gal}(K/F)$ .

Via this homomorphism, the preimage of  $\tau$  is the equivalence class of  $\sigma$ .

See **Theorem 4** in (Pinter, 1990, p. 330).

Therefore, the norm of  $\alpha$  with respect to  $K/F$  is  $\alpha \sigma|_K(\alpha)$ .

By (1) above,  $\alpha \sigma|_K(\alpha) = N_{K/F}(\alpha) = -1$ .  $\square$

## PART 2

Let  $\alpha \in K$  be an element with norm  $N_{K/F}(\alpha) = -1$ .

Show that there exists a cyclic extension  $L/F$  of degree 4.

*Hint:* The case when  $\alpha \in F$  must be treated separately.

When  $\alpha \notin F$ , try  $L = K[\sqrt{1 + \alpha^2}]$ .

## SOLUTION 1.2.2

The element  $\alpha$  is of the form  $x + \sqrt{a}y$  for some  $x, y \in F$ . First, suppose  $\alpha \in F$ :

We have  $y = 0$ . Since  $N_{K/F}(\alpha) = -1$ , we also have  $x^2 = -1$ .

This implies that  $i = \sqrt{-1} \in F$ . So  $F$  contains a primitive  $4^{\text{th}}$  root of unity:

Therefore we may apply *The Fundamental Theorem of Kummer Theory*:

Subgroups of order  $n \geq 1$  in  $F^\times / F^{\times n}$  give rise to Galois extensions of degree  $n$ .

Let  $[b]$  be such a subgroup. Let  $L/F$  be such an extension.

Then  $L$  is generated as  $F[\sqrt[n]{b}]$  for any  $b$  in  $[b]$ .

See **Theorem 1.25** in (Guillot, 2018, p. 14) for details.

It suffices to show that such a subgroup and generating element exist for  $n = 4$ .

Before we do so, observe that the exponent of  $F^\times / F^{\times 4}$  is 4. (2)

Every element of  $[b]$  is of the form  $bf^4$  for some  $b \in F^\times \setminus F^{\times 4}$  and  $f \in F^\times$ .

Furthermore,  $bf^4$  is in lowest terms, so that  $b$  does not contain a  $4^{th}$  power.

Let  $m$  be the order of  $[b]$  in  $F^\times/F^{\times 4}$ . If  $m > 4$ , there exists some  $c = (bf^4)^m \in F^{\times 4}$ .

This implies that  $b^m = b^{m-4}b^4 = 1$ , contradicting that  $c$  is given in lowest terms.

By group theory, the order of any subgroup  $[b]$  in  $F^\times/F^{\times 4}$  must divide the exponent 4.

Now it is clear that we may choose  $b = a$  and  $[b] = [a]$ :

Since  $a$  is not a square or a  $4^{th}$  power in  $F^\times$ , the order of  $[a]$  cannot be 2 or 1. (3)

So the order of  $[a]$  is 4, and a cyclic extension  $L/K$  of degree 4 exists.

Now suppose  $\alpha \notin F$ . We take Guillot's hint and try  $L = K[\sqrt{1 + \alpha^2}]$ .

Clearly,  $K/F$  is Galois of degree 2 with  $\mathbf{Gal}(K/F) \cong C_2$ .

Let  $\sigma$  be the non-identity (conjugation) and  $\bar{\alpha} = \sigma(\alpha)$ .

We have:  $N_{K/F}(1 + \alpha^2) = (1 + \alpha^2)(1 + \sigma(\alpha)^2) = (1 + \alpha^2)(1 + \bar{\alpha}^2)$ .

Recall that  $N_{K/F}(\alpha) = \alpha\sigma(\alpha) = -1$ , and so  $\alpha^2\sigma(\alpha)^2 = 1$ .

Applying these "formulae", we get  $N_{K/F}(1 + \alpha^2) = (\alpha - \bar{\alpha})^2$ .

If  $1 + \alpha^2$  lies in  $K^{\times 2}$ , then  $N_{K/F}(1 + \alpha^2) = N_{K/F}(\beta)^2$  for some  $\beta \in K$ .

But  $N_{K/F}(\beta) \in F$ , which implies that  $N_{K/F}(1 + \alpha^2)$  also lies in  $F^{\times 2}$ .

This cannot be the case since  $(\alpha - \sigma(\alpha))^2 = 4y^2a$  does not lie in  $F^{\times 2}$ .

While  $4y^2$  is a square, recall that we have assumed  $a \notin F^{\times 2}$ .

Therefore,  $1 + \alpha^2$  is not a square in  $K^\times$ .

We may now apply the so-called *Equivariant Kummer Theory*:

Clearly,  $L/K$  is Galois of degree 2 with  $\mathbf{Gal}(L/K) \cong C_2$ .

Suppose that  $K$  contains a primitive  $n^{th}$  root of unity.

Consider subgroups of order  $n \geq 1$  in  $K^\times/K^{\times n}$  fixed by the action of  $\mathbf{Gal}(K/F)$ .

These give rise to Galois extensions  $L/K$  of degree  $n$  such that  $L/F$  is also Galois.

Let  $[b]$  be such a subgroup of  $K^\times/K^{\times n}$ . Then  $L$  is generated as  $K[\sqrt[n]{b}]$  for any  $b$  in  $[b]$ .

See **Theorem 1.26** in (Guillot, 2018, p. 14) for details.

Certainly,  $K$  contains the primitive *square* root of unity, namely  $-1$ .

Using (2) and (3) above, the order of  $[1 + \alpha^2]$  in  $K^\times/K^{\times 2}$  is 2.

It remains to show that  $[1 + \alpha^2]$  is preserved by the action of  $\mathbf{Gal}(K/F)$  :

$$\sigma(1 + \alpha^2) = 1 + \bar{\alpha}^2 = \frac{N_{K/F}(1 + \alpha^2)}{1 + \alpha^2} = \frac{4y^2\alpha}{1 + \alpha^2} = (1 + \alpha^2) \cdot \left( \frac{2y\sqrt{\alpha}}{1 + \alpha^2} \right)^2.$$

Thus,  $\sigma(1 + \alpha^2) = (1 + \alpha^2) \cdot k^2$  for  $k = \left( \frac{2y\sqrt{\alpha}}{1 + \alpha^2} \right)^2 \in K^\times$ , and  $\sigma$  fixes  $[1 + \alpha^2]$ .  $\square$

### PART 3

Show that the following are equivalent:

- (a) There exists an  $\alpha \in K$  with  $N_{K/F}(\alpha) = -1$ , and
- (b)  $a$  is a sum of two squares in  $F$ .

#### SOLUTION 1.2.3

Recall that  $F$  is a field of characteristic  $p \neq 2$  and  $K = F[\sqrt{a}]$ .

Clearly,  $K/F$  is Galois of degree 2 with  $\mathbf{Gal}(K/F) \cong C_2$ .

Let  $\sigma$  be the non-identity (conjugation) which sends  $\sqrt{a}$  to  $-\sqrt{a}$ .

If  $a = x^2 + y^2$  for some  $y \neq 0$  and  $x$  in  $F$ , then  $\frac{x^2 - a}{y^2} = -1$ . Also,

$$\frac{x + \sqrt{a}}{y} \cdot \frac{x - \sqrt{a}}{y} = \frac{x + \sqrt{a}}{y} \cdot \sigma\left(\frac{x + \sqrt{a}}{y}\right) = -1.$$

Letting  $\alpha = \frac{x + \sqrt{a}}{y} \in K$ , the equation above reduces to  $N_{K/F}(\alpha) = -1$ .

On the other hand, if  $y = 0$ , then  $a = x^2$ . This cannot be the case because  $a \notin F^{\times 2}$ .

Therefore (b)  $\implies$  (a).

Every element of  $K$  is of the form  $x + \sqrt{a}y$  for some  $x, y \in F$ .

If  $N_{K/F}(\alpha) = -1$ , then  $(x + \sqrt{a}y) \cdot (x - \sqrt{a}y) = x^2 - ay^2 = -1$ .

If  $y = 0$ , then  $a = x^2$ . This cannot be the case because  $a \notin F^{\times 2}$ .

So we can safely rearrange  $x^2 - ay^2 = -1$  as  $a = \left(\frac{1}{y}\right)^2 + \left(\frac{x}{y}\right)^2$ .

Therefore (a)  $\implies$  (b).  $\square$

## REFERENCES

- Guillot, P. (2018). *A Gentle Course in Local Class Field Theory: Local Number Fields, Brauer Groups, Galois Cohomology*. Cambridge: Cambridge University Press.
- Morandi, P. (1996). *Field and Galois Theory*. Graduate Texts in Mathematics, vol 167. Springer, New York, NY.
- Pinter, C.C. (1990) *A Book of Abstract Algebra*. 2nd Edition, Dover Publications, Inc., Mineola, New York.