PROBLEM 1.3 (Guillot, 2018, p. 21)

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

Suppose the equation $x^2 - y^2 = 1$ has a solution with $x, y \in F$.

Let H be a subgroup of D_8, the dihedral group of order 8.

Show that there exists a Galois extension L/F such that:

- $F[\sqrt{a}, \sqrt{b}] \subset L$, and
- $\mathbf{Gal}(L/F) \cong H$.

SOLUTION 1.2.1

This problem is a generalization of **Proposition 1.28** in (Guillot, 2018, p. 16).

Here we do not assume that $[a]$ and $[b]$ are linearly independent classes in $F^\times/F^{\times 2}$.

As a result $\mathbf{Gal}(L/F) \cong H$ rather than $\mathbf{Gal}(L/F) \cong D_8$.

As Guillot hints, there are many possibilities to consider here.

These arise in part due to the different ways in which $[a]$ and $[b]$ can be dependent:

First, note that $F^\times/F^{\times 2}$ is a vector space over $\mathbb{Z}/2\mathbb{Z}$.

The scalars are either 0 or 1. The vectors are classes such as $[a]$ and $[b]$.

These vectors form an abelian group under *multiplication* (not addition).

Accordingly, the scalar operation is really *exponentiation* (not multiplication).

For example, consider $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, which is also a vector space over $\mathbb{Z}/2\mathbb{Z}$.

The scalars are again 0 or 1. The vectors are classes $[p]$ for prime p and $[-1]$.

Indeed, every element of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ can be written as $\pm p_1^{n_1} p_2^{n_2} p_3^{n_3} ...$ where the n_k are 0 or 1.

Thus, we interpret the dependence of $[a]$ and $[b]$ as follows:

There exist scalars $c, d \in \mathbb{Z}/2\mathbb{Z}$ not both 0 such that $[a]^c = [b]^d$.

So $[a]$ and $[b]$ can be linearly dependent if either equals $[1]$ or if $[a] = [b]$.

This is an application of **Example 1.4** in (Guillot, 2018, pp. 4-5).

PART 1: The case when $[a] = [1] = [b]$.

PART 2: The case when $[a] \neq [1] = [b]$.

PART 3: The case when $[a] = [1] \neq 1$.

PART 4: The case when $[a] = [b] \neq 1$.

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.