

# 1 Galois Theory

## Problem 1

Let  $F$  be a field of prime characteristic  $p$ . Suppose  $E = F(\alpha)$  such that  $\alpha \notin F$  but  $\alpha^p - \alpha \in F$ .

1. Find  $[E : F]$ .
2. Prove that  $E/F$  is a Galois extension.
3. Find the Galois group  $\text{Gal}(E/F)$ .

**Hint:** Note that  $(x + 1)^p - (x + 1) = x^p - x$ .<sup>a</sup>

<sup>a</sup>This is the Artin-Schreier polynomial.

*Proof.*

1. This is the hardest part: Let's denote  $b = \alpha^p - \alpha \in F$ . Consider the polynomial

$$f(x) = x^p - x - b.$$

Clearly from the hint, we can see that  $\alpha + k, k = 0, 1, \dots, p-1$  are roots of  $f(x)$ . They are all distinct. Thus

$$f(x) = \prod_{k=0}^{p-1} (x - \alpha - k)$$

If this polynomial is reducible over  $F$ , then there exists  $n < p$  such that

$$g(x) = \prod_{i=0}^{n-1} (x - \alpha - k_i) \in F[x]$$

But this implies that the coefficient of  $x^{n-1}$  in  $g(x)$  is

$$n\alpha + k_0 + k_1 + \dots + k_{n-1} \in F$$

which implies  $\alpha \in F$ , a contradiction. Thus  $f(x)$  is irreducible over  $F$ .

2. This follows immediate from part 1 that  $f$  is irreducible and has  $p$  distinct roots. Thus the splitting field of  $f$  is  $E$  and  $E = F(\alpha)$  is separable as  $\alpha$  is separable over  $F$ . Thus  $E/F$  is a Galois extension.
3. The Galois group is a group of order  $p$ , thus it is isomorphism to  $\mathbb{Z}/p\mathbb{Z}$ .

Hence we are done. □

## Problem 2

Let  $\zeta := e^{2\pi i/7}$  be a primitive 7th root of unity. Let  $K = \mathbb{Q}(\zeta)$ .

1. Prove that there exists an element  $\alpha \in K$  such that  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ .
2. Express  $\alpha$  in terms of  $\zeta$ .

*Proof.* We will prove two items at once. Consider the element given by

$$\alpha = \zeta + \zeta^2 + \zeta^4$$

Then it can be seen that the map  $\sigma$  such that  $\sigma(\zeta) = \zeta^3$  generates the Galois group of the cyclotomic field. This implies the desired field extension will correspond to the fixed field of the subgroup generated by  $\sigma^2$ . We can see that the  $\alpha$  defined as above is fixed by  $\theta = \sigma^2$ . Indeed

$$\theta(\alpha) = \sigma^2(\zeta + \zeta^2 + \zeta^4) = \zeta^9 + \zeta^4 + \zeta^{36} = \zeta^2 + \zeta^4 + \zeta = \alpha$$

Clearly  $\alpha \notin \mathbb{Q}$ , since  $\zeta$  has degree 6 over  $\mathbb{Q}$ . Moreover,  $\alpha$  can't have degree 3 over  $\mathbb{Q}$ , otherwise it is inside the intersection of two intermediate fields of degree 2 and 3, thus is rational. Hence we can conclude that this is the desired element.

Another way to do this problem is as follows. We have

$$\alpha^2 = \zeta^2 + \zeta^4 + \zeta + 2(\zeta^3 + \zeta^6 + \zeta^5) = \zeta^2 + \zeta^4 + \zeta - 2(1 + \zeta^2 + \zeta^4 + \zeta) = -2 - \alpha$$

Thus we have the polynomial  $x^2 + x + 2$  which is irreducible over  $\mathbb{Q}$ , since it has no rational roots. Thus we can conclude that  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ .

$$\alpha^2 + \alpha + 2 = 0$$

This yields the desired element  $\alpha$ . □

**Remark:** A Sage code for this problem is given below.

```
k = CyclotomicField(7); k
zeta=k.gen(); a = zeta+zeta^2+zeta^4
a.minpoly()
```

### Problem 3

Let  $K$  be a finite field of characteristic  $p$  with  $p^k$  elements. Suppose that  $F, L$  are subfields of  $K$  with  $|F| = p^n$  and  $|L| = p^m$ . Also, suppose that  $|F \cap L| = p$ . Prove that  $K = FL$  if and only if  $nm = k$ .

*Proof.* Since every finite extension of a finite field is Galois, and we have that

$$\text{Gal}(FL/F) \cong \text{Gal}(L/L \cap F) = m$$

In particular, we have  $[FL : F] = m$ . Thus

$$[FL : L \cap F] = [FL : F][F : L \cap F] = mn$$

Hence  $K = FL$  if and only if  $mn = k$ . □

### Problem 4

Let  $E$  be a Galois extension of  $\mathbb{Q}$  of order 2022. Show that there exists a cubic polynomial  $f \in \mathbb{Q}[x]$  such that  $f$  is irreducible and has 3 distinct roots in  $E$ .

*Proof.* Note that we have

$$2022 = 337 \times 2 \times 3$$

**to be added** □

## 2 Group theory

<sup>1</sup>We can also prove this by using the uniqueness of finite extension of finite field of given order.

**Problem 5**

Let  $G$  be a finite group and  $H$  be a proper subgroup. Suppose that  $\gcd(|H|, [G : H]) > 1$ . Show that there exists some  $g \in G \setminus H$  such that  $gHg^{-1} \cap H \neq \{e\}$ .

*Proof.*<sup>2</sup> Anyway, one way to think about this problem is to consider the action of  $H$  on  $G/H$  by left multiplication.

The stabilizer of an element  $gH \in G/H$  is equal to

$$\begin{aligned}\{h \in H : hgH = gH\} &= \{h \in H : g^{-1}hgH = H\} \\ &= \{h \in H : g^{-1}hg \in H\} \\ &= \{h \in H : h \in gHg^{-1}\} \\ &= gHg^{-1} \cap H,\end{aligned}$$

so we simply wish to show that some element of  $G/H$ , besides the trivial coset  $eH$ , has nontrivial stabilizer.

Well, suppose for contradiction that this is not the case, i.e. the stabilizer of  $gH$  is  $\{e\}$  whenever  $g \notin H$ . Then by the orbit-stabilizer theorem we have at most two types of orbits in the  $H$ -set  $G/H$ :

- A single orbit of cardinality 1, namely  $\{eH\}$ .
- Some number (say,  $n$ ) of orbits of cardinality  $|H|$

Since every  $H$ -set is the disjoint union of its orbits, we conclude that

$$[G : H] = |G/H| = 1 + n|H|$$

for some integer  $n \geq 0$ . This implies that  $\gcd(|H|, [G : H]) = 1$ , which is a contradiction.  $\square$

<sup>2</sup>this solution is originally asked by me here: <https://math.stackexchange.com/a/5063992/1231540>

**Problem 6**

Given  $z = -1 + i$ , show that

$$2^n + 1 - z^n - \bar{z}^n$$

is an integral multiple of 5.

*Proof.* First we make an elementary observation

$$z^8 = \bar{z}^8 = 16 \equiv 1 \pmod{5}$$

So, to check for the remainder when divided by 5 of  $z^n + \bar{z}^n$ , it is sufficient to look for the first seven values modulo 5. Let's look at the table

n	0	1	2	3	4	5	6	7
$z^n + \bar{z}^n \pmod{5}$	2	3	0	4	2	3	0	4

From the table, we can see a finer description - it is enough to consider  $n$  modulo 4 to find the remainder when divided by 5. From Fermat's little theorem, for  $n = 4k + l$  with  $0 \leq l \leq 3$

$$2^n + 1 \equiv 2^l + 1 \pmod{5}$$

It is easy to check that

1	0	1	2	3
$2^l + 1 \pmod{5}$	2	3	0	4

The two tables have the same values for  $n$  modulo 4, thus the given expression must be divisible by 5.  $\square$