

## WORKSHOP 2

2024 ALGEBRA 2

### 1. FACTORISATION IN A FINITE FIELD

The polynomial  $f(x) = x^3 + x + 1 \in \mathbf{F}_5[x]$  is irreducible. Let  $K = \mathbf{F}[t]/(f(t))$ . Find the irreducible factorisation of  $f(x)$  in  $K[x]$ .

**1.1. Solution sketch.** We know that  $t \in K$  is a root of  $f(x)$ . We can find the other roots by applying the Frobenius, so  $t^3$ , and  $t^9$ . So,

$$f(x) = (x - t)(x - t^3)(x - t^9).$$

Can you bring the roots in the “reduced form” (at most quadratics in  $t$ )?

### 2. CONJUGATES

Let  $F \subset K$  be a field extension. We say that  $\alpha, \beta \in K$  are *conjugates* over  $F$  if they have the same minimal polynomial over  $F$ .

Let  $K$  be a finite field of characteristic  $p$ . Let  $\phi: K \rightarrow K$  be the Frobenius map.

- (1) Prove that the conjugates of  $a \in K$  are  $a, \phi(a), \phi^2(a), \dots$ .
- (2) Deduce that the degree of  $a$  over  $\mathbf{F}_p$  is the smallest  $n$  such that  $\phi^n(a) = a$ .
- (3) More generally, let  $K \subset L$  be an extension of finite fields with  $|K| = p^n$ . Prove that the conjugates of  $a \in L$  over  $K$  are  $a, \phi^n(a), \phi^{2n}(a), \dots$ .
- (4) What is the analogue of (2) in this situation?

#### 2.1. Solution sketch.

- (1) Suppose  $f(x) = \sum a_i x^i$  is the minimal polynomial of  $a$ , where  $a_i \in \mathbf{F}_p$ . By applying the Frobenius map, we see that

$$\phi\left(\sum a_i a^i\right) = \sum a_i \phi(a)^i = 0,$$

so  $f(\phi(a)) = 0$ . So  $\phi(a)$  also has the same minimal polynomial.

To see that these are *all* the conjugates, let  $n$  be the smallest such that  $\phi^n(a) = a$ . Then  $a, \phi(a), \dots, \phi^{n-1}(a)$  are distinct. Consider

$$f(x) = (x - a) \cdots (x - \phi^{n-1}(a)) \in K[x].$$

We see that  $\phi(f) = f$ , so  $f \in \mathbf{F}_p[x]$ . In fact, this must be the minimal polynomial of  $a$  (do you see why?). So the  $\phi^i(a)$  are indeed all the conjugates of  $a$ .

- (2) Follows from what we did in (1).
- (3) This is very similar. The key idea is that  $a \in L$  lies in  $K$  if and only if  $\phi^n(a) = a$ .
- (4) The degree of  $a \in L$  over  $K$  is the smallest  $m$  such that  $\phi^{nm}(a) = a$ .

### 3. FACTORISATION, ONCE AGAIN

Let  $f(x) \in \mathbf{F}_p[x]$  be irreducible of degree 18. Let  $\mathbf{F}_p \subset K$  be an extension of degree 4. How does  $f(x)$  factorise in  $K[x]$ ?

**Hint.** Let  $K \subset L$  be an extension of degree 9, so that  $\mathbf{F}_p \subset L$  is of degree 36. First factorise  $f(x)$  in  $L$  and then “collect the conjugates” over  $K$ .

**3.1. Solution sketch.** Let  $a \in L$  be a root of  $f(x)$ . Then 18 is the smallest such that  $\phi^{18}(a) = a$  and the factorisation of  $f(x)$  is

$$(x - a)(x - \phi(a)) \cdots (x - \phi^{17}(a)).$$

The conjugates of  $t \in L$  over  $K$  are  $t, \phi^4(t), \phi^8(t), \dots$ . So, the 18 roots  $\phi^i(a)$  split into two sets of conjugates over  $K$ , namely  $\phi^i(a)$  for  $i$  even and for  $i$  odd. This means that  $f(x) \in K[x]$  factorises into a degree 9 irreducible (whose roots are the first set) and another degree 9 irreducible (whose roots are the second set).