GALOIS THEORY
Solutions to Worksheet 9

A 1. (a) The two polynomials have degree 3 and have no roots in $\mathbb{F}_2$ (just plug $x = 0, 1$) hence they are irreducible.

If $\sigma\colon K \to L$ then $\sigma(\alpha)$ is a root of $f(X)$ in L; and $f(X)$ has three roots in L:

$$\beta + 1; \quad \beta^2 + 1; \quad \beta^2 + \beta$$

indeed, for example, we can check directly that:

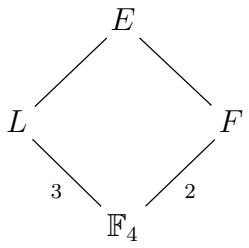
$$(\beta+1)^3 = \beta^3 + \beta^2 + \beta + 1 = (\beta^2+1) + \beta^2 + \beta + 1 = \beta = (\beta+1) + 1$$

that is, $\beta + 1$ is a root of $f(x)$. The other roots of f are $\mathrm{Fr}_2(\beta+1) = \beta^2 + 1$ and $\mathrm{Fr}_2(\beta^2+1) = \beta^4 + 1 = \beta(\beta^2+1) + 1 = \beta^2 + 1 + \beta + 1 = \beta^2 + \beta$. (But one can also check directly.)

A basic result about fields states that a morphism from K to L is the same as a root of $f(X)$ in L and there are 3 of these. As f and g are irreducible we know that K and L have degree 3 over $\mathbb{F}_2$ and we have shown that any two finite fields of the same degree over the base field are isomorphic. Since both fields have degree 3 over the base field $\mathbb{F}_2$, all morphisms from K to L are isomorphisms hence there are 3 of these. (This gives another reason why K and L are isomorphic.)

(b) $h(X) \in \mathbb{F}_2[X]$ is irreducible because: it has no roots (plug $X = 0$ and $X = 1$) in $\mathbb{F}_2$ AND it is not divisible by $X^2 + X + 1$, the only irreducible degree two polynomial in $\mathbb{F}_2[X]$ — as can be checked by performing long division in $\mathbb{F}_2[X]$.

Let $L \subset E$ be the splitting field of $h(X)$ as a polynomial in $L[X]$. The extension $\mathbb{F}_2 \subset E$ is normal and separable because ALL finite extensions of finite fields are. Clearly E contains the splitting field $\mathbb{F}_2 \subset F$ of $h(X) \in \mathbb{F}_2[X]$:



We know that $h(X) \in \mathbb{F}_2[X]$ is irreducible; hence if $\gamma \in F$ is a root of h, then $[\mathbb{F}_2(\gamma) : \mathbb{F}_2] = 4$. We know that every finite extension of a finite field is normal and separable, therefore $\mathbb{F}_2 \subset F$ is normal and hence (by a known characterisation of normal extensions) $h(X)$ splits completely in $\mathbb{F}_2(\gamma)[X]$ — because it is irreducible over $\mathbb{F}_2$ and has a root in $\mathbb{F}_2(\gamma)$ — hence actually $F = \mathbb{F}_2(\gamma)$ and then, as indicated in the diagram, $[F : \mathbb{F}_2] = [\mathbb{F}_2(\gamma) : \mathbb{F}_2] = 4$.

The tower law implies that $3|[E : \mathbb{F}_2]$ and $4|[E : \mathbb{F}_2]$ hence $12|[E : \mathbb{F}_2]$. But clearly also $E = L(\gamma)$ and then $[E : L]$ is the degree of the minimal polynomial of γ over L, which is a factor of h, hence $[E : \mathbb{F}_2] = [E : L][L : \mathbb{F}_2] \leq 12$. So in fact $[E : \mathbb{F}_2] = 12$; $[E : L] = 4$, $h \in L[X]$ is the minimal polynomial of γ and it is therefore irreducible.

A 2. (This is a pure algebra question.) The $(n-1)$-cycle c must fix an element of $[n]$[1] which we may well assume to be 1, and then after re-labelling the elements of $[n]$ we may assume that $c = (23 \dots n)$. Let t be the transposition; then:

Either t involves 1, and then by further relabelling elements we may assume $c = (23 \cdots n)$, $t = (12)$, and it is easy to conclude from here;

Or $t = (ab)$ where $1 < a < b$: this is what we assume from now on.

Because G is transitive, it must contain an element σ such that $\sigma(a) = 1$, but then $\sigma t \sigma^{-1} = (1\sigma(b))$ and we are back in the previous case.

A 3. We look at the polynomial modulo small primes: Modulo $p = 2$ we get:

$$f(X) = X^6 - 12X^4 + 15X^3 - 6X^2 + 15X + 12 \equiv X(X^5 + X^2 + 1) \mod 2$$

where the second polynomial $r(X) = X^5 + X^2 + 1$ is irreducible because if it weren't it would split an irreducible degree two polynomial, but the only such polynomial is $X^2 + X + 1$ which does not divide into $r(X)$ (direct inspection). By Corollary 57, the Galois group G contains a 5-cycle.

Eisenstein at $p = 3$ shows that $f(X)$ is irreducible in $\mathbb{Q}[x]$ and in turn this implies that G is transitive.

Next:

$$f(X) \equiv (X + 1)(X + 2)(X + 3)(X + 4)(X^2 + 3) \mod 5$$

thus by the theorem in the footnote G contains a transposition.

By the previous question $G = \mathfrak{S}_6$.

A 4. (a) Let us first consider the polynomial in $\mathbb{F}_2[X]$. Clearly $X = 1$ is a root of $f(X)$ and a small calculation shows

$$X^4 + X^2 + X + 1 = (X + 1)(X^3 + X^2 + 1) \quad \text{in} \quad \mathbb{F}_2[X]$$

and then $X^3 + X + 1 \in \mathbb{F}_2[X]$ is irreducible because it has no roots in $\mathbb{F}_2$ (just plug in $X = 0$ and $X = 1$).

[1]Notation: $[n] = \{1, 2, \dots, n\}$ is the set with n elements.

Next, we work in $\mathbb{F}_3[X]$. A quick inspection shows that $f(X)$ has no roots in $\mathbb{F}_3$: just plug $X = 0, 1, -1$. To show that the polynomial $f(X) \in \mathbb{F}_3[X]$ is irreducible, we show that it is not divisible by any of the three irreducible degree 2 polynomial in $\mathbb{F}_3[X]$: these are:

$$X^2 + 1, \quad X^2 + X - 1, \quad X^2 - X - 1$$

Performing three long divisions in $\mathbb{F}_3[X]$ we see:

$$\begin{aligned} X^4 + X^2 + X + 1 &= (X^2 + 1)(X^2) + X + 1 \\ X^4 + X^2 + X + 1 &= (X^2 + X - 1)(X^2 - X) + 1 \\ X^4 + X^2 + X + 1 &= (X^2 - X - 1)(X^2 + X) - X + 1 \end{aligned}$$

these calculations show that f is irreducible in $\mathbb{F}_3[X]$.

(b) By Corollary 57 the Galois group G of the splitting field $\mathbb{Q} \subset K$ contains a 3-cycle and a 4-cycle. If a subgroup G of $\mathfrak{S}_4$ contains a 3-cycle and a 4-cycle then $G = \mathfrak{S}_4$. (See the question below.) Therefore, $G = \mathfrak{S}_4$.

A 5. (a) First, working modulo 2,

$$f(X) \equiv X^4 + 3X + 1 \in \mathbb{F}_2[X]$$

is irreducible. Indeed, by inspection, it does not have a root in $\mathbb{F}_2$, and it is not divisible by the only irreducible degree 2 monic polynomial $X^2 + X + 1 \in \mathbb{F}_2[X]$. In fact long division gives

$$X^4 + X + 1 = (X^2 + X + 1)(X^2 + X) + 1$$

Next, it is easy to factor $f(X)$ mod 5:[2]

$$f(X) \equiv (X - 1)(X^3 + X^2 + X - 1) \in \mathbb{F}_5[X]$$

where the degree 3 factor is irreducible because, by inspection, it has no root in $\mathbb{F}_5$.

(b) Suppose that $G \subset \mathfrak{S}_4$ contains a 4-cycle and a 3-cycle. Let the 4-cycle be $s = (abcd)$. Note that we can write $s = (dabc)$, etc. Thus, we may assume that the 3-cycle t fixes the last letter d in the 4-cycle. Now either $t = (abc)$ or $t = (acb)$, but then $t^2 = (abc)$. The conclusion is that we may assume $s = (1234)$, $t = (123)$. You take it from here.

(c) By Part (a) and the theorem in the footnote, the Galois group contains a 4-cycle and a 3-cycle hence, by Part (b) it must be all of $\mathfrak{S}_4$.

A 6. With all the hints and the examples, this should not be too hard. You do it (or else ignore this question).

[2]Working mod 3 is not going to lead to useful information: it is clear by inspection that $f(X)$ has no root in $\mathbb{F}_3$ and then either $f(X)$ is irreducible (no useful conclusion) or it splits into two quadratic polynomials (again no useful conclusion).