Exercise 1. Let p be a prime number and $f(X) = X^4 + pX + p$.

(a) Compute $R_f(X)$ and $D(f)$. Conclude that the zeros of $R_f(X)$ satisfy $Z_R \subset \{\pm 1, \pm p, \pm p^2\}$. Check that ± 1 and $\pm p^2$ are not roots of $R_f(X)$ for any p, but $R_f(p) = p^2(p-5)$ and $R_f(-p) = p^2(p-3)$. Conclude that $R_f(X)$ has a root in Q if and only if $p = 3, 5$.

(b) Prove that $G_f = S_4$ if $p \neq 3, 5$.

(c) If $p = 3$, prove that $G_f = D_4$.

(d) If $p = 5$, prove that $G_f = C_4$.

SOLUTION: (a) We get $R_f(X) = X^3 - 4pX - p^2$, $\mathrm{Disc}(f) = p^3(256 - 27p)$. The rest is clear from this.

(b) is a consequence of (a), since $p^3(256 - 27p)$ is never a perfect square and $R_f(X)$ is irreducible in $\mathbb{Q}[X]$ when $p \neq 3, 5$.

(c) If $p = 3$, then $R_f(X) = (X + 3)(X^2 - 3X - 3)$. Thus the splitting field M of $R_f(X)$ over $\mathbb{Q}$ is $\mathbb{Q}\sqrt{21})$. Since $X^4 + 3X + 3$ is irreducible over $\mathbb{Q}(\sqrt{21})$, $G_f = D_4$.

(d) Now let $p = 5$. The resolvent cubic is

$$R_f(X) = X^3 - 20X - 25 = (X - 5)(X^2 + 5X + 5) = \left(X - \frac{5 - \sqrt{5}}{2}\right)\left(X - \frac{5 + \sqrt{5}}{2}\right).$$

Thus, its splitting field M is $\mathbb{Q}[\sqrt{5}]$. Since

$$X^4 + 5X + 5 = \left(X^2 + \sqrt{5}X + \frac{5 - \sqrt{5}}{2}\right)\left(X^2 + \sqrt{5}X + \frac{5 + \sqrt{5}}{2}\right) \in \mathbb{Q}[\sqrt{5}][X],$$

we conclude that $G_f = C_4$. □

Exercise 2. (a) List all irreducible polynomials of degree 2 in $\mathbb{F}_5[X]$.

(b) Let $\mathbb{F}_5[X]/(X^2 + 3) = \mathbb{F}_5[\alpha]$, $\mathbb{F}_5[X]/(X^2 + 2) = \mathbb{F}_5[\beta]$ and $\mathbb{F}_5[X]/(X^2 + X + 1) = \mathbb{F}_5[\gamma]$. Construct explicit isomorphisms $\mathbb{F}_5[\alpha] \xrightarrow{\varphi} \mathbb{F}_5[\beta] \xrightarrow{\psi} \mathbb{F}_5[\gamma]$.

(c) Find a generator g for $\mathbb{F}_5[\alpha]^\times$, and use g and the isomorphisms φ and ψ found in (b) to produce generators of $\mathbb{F}_5[\gamma]^\times$ and $\mathbb{F}_5[\beta]^\times$.

SOLUTION: The polynomials of degree 2 irreducible in $\mathbb{F}_5[X]$ are X^2+2, X^2+3, X^2+X+1, $X^2 + X + 2$, $X^2 + 2X + 3$. $X^2 + 2X + 4$, $X^2 + 2X + 3$, $X^2 + 2X + 2$, $X^2 + 4X + 1$ y $X^2 + 4X + 2$ (to find them, it suffices to compute its complementary set, formed by those polynomials which are a product of two polynomials of degree 1).

(b) Since $\alpha^2 = 2 \in K_1$, necessarily $\varphi(\alpha)^2 = 2 \in K_2$. Thus, candidates for $\varphi(\alpha)$ are elements $a + b\beta \in \mathbb{F}_5[\beta]$ with $(a + b\beta)^2 = 2$. We look for them.

$$(a + b\beta)^2 = 2 \Leftrightarrow a^2 + 2ab\beta + b^2\beta^2 = 2 \Leftrightarrow a^2 + 3b^2 + 2ab\beta = 2$$

$$\Leftrightarrow \begin{cases} a^2 + 3b^2 = 2 \\ 2ab = 0 \end{cases} \Leftrightarrow \begin{cases} a = 0,\ b = \pm 2 \\ b = 0, a^2 = 2, \text{impossible} \end{cases}$$

We thus have two possible isomorphisms φ between $\mathbb{F}_5[\alpha]$ and $\mathbb{F}_5[\beta]$:

$$\alpha \mapsto 2\beta, \quad \text{or } \alpha \mapsto -2\beta.$$

Analogously, in order to construct an isomorphism $\psi : \mathbb{F}_5[\beta] \to \mathbb{F}_5[\gamma]$, since $\beta^2 = 3$, its image must be an element $a + b\gamma \in \mathbb{F}_5[\gamma]$ such that $(a + b\gamma)^2 = 3$. Let us look for it.

$$(a+b\gamma)^2 = 3 \Leftrightarrow a^2 + 2ab\gamma + b^2\gamma^2 = 3 \Leftrightarrow a^2 + 4b^2 + (2ab + 4b^2)\gamma = 3$$

$$\Leftrightarrow \begin{cases} a^2 + 4b^2 = 3 \\ 2b(a+2b) = 0 \end{cases} \Leftrightarrow \begin{cases} a = 3b,\ 3b^2 = 3 \Rightarrow b = \pm 1, a = 3b \\ b = 0, a^2 = 3, \text{impossible} \end{cases}$$

We thus have two options for isomorphisms ψ between K_1 and K_2:

$$\beta \mapsto 3 + 3\gamma, \quad \text{or } \beta \ \mapsto -3 - 3\gamma.$$

(c) Doing the computations, we get that $g = 1+3\alpha$ is a generator, that is, $\mathbb{F}_5[\alpha]^\times = \langle 1+3\alpha \rangle$. Its possible images $1 + 3\varphi(\alpha) = \begin{cases} 1+\alpha \\ 1-\alpha \end{cases}$ are generators of $\mathbb{F}_5[\beta]^\times$. Analogously, its possible images under $\psi \circ \varphi$,

$$(\psi \circ \varphi)(1+3\alpha) = \begin{cases} 1 + \psi(\beta) = 4 + 3\gamma, -2 - 3\gamma \\ 1 - \psi(\beta) = -2 - 3\gamma, 4 + 3\gamma \end{cases} = \begin{cases} 4 + 3\gamma \\ -2 - 3\gamma \end{cases}$$

are generators of $\mathbb{F}_5[\gamma]^\times$. □

Exercise 3. Let $f(X)$ be a polynomial of degree 6 in $\mathbb{F}_5[X]$, and let $K = \mathbb{F}_5[X]/(f)$. How many elements $\alpha \in K$ satisfy $K^\times = \langle \alpha \rangle$? How many elements $\beta \in K$ satisfy $K = \mathbb{F}_5[\beta]$?

SOLUTION Since $|K| = 5^6 = 15625$, we know that $K^\times$ is a cyclic group of order

$$5^6 - 1 = 15624 = 2^3 \cdot 3^2 \cdot 7 \cdot 31.$$

Let φ be Euler's function. The number of generators of a cyclic group of order 15624 is

$$\varphi(15624) = \varphi(8)\varphi(3^2)\varphi(7)\varphi(30) = 4 \cdot 6 \cdot 6 \cdot 30 = 4320.$$

Thus, exactly 4320 elements in K generate $K^\times$. On the other hand, the number of elements $\beta \in K$ with $K = \mathbb{F}_5[\beta]$ equals the number of elements in K which are not $\mathbb{F}_5$, $\mathbb{F}_{5^2}$ or $\mathbb{F}_{5^3}$. Since $\mathbb{F}_{5^2} \cup \mathbb{F}_{5^3} = \mathbb{F}_5$, there are $4320 - 125 - 25 + 5 = 4275$ of them.

Exercise 4. Let $K = \mathbb{F}_{3^n}$, with $n \geq 2$.
(a) How many elements have their square in K?
SOLUTION: The elements of K which have a square in K are 0 and the even powers of any generator.

(b) Prove that the product P of all elements of $K^\times$ equals 2.
SOLUTION: Let $P = \prod_{x \in K^\times} x$. Since the product is conmutative, every element $x \in K^\times$ can be paired with its inverse $x^{-1} \neq x$, except for the only element of order 2, which is 2.

(c) Prove that the additive group $(K, +)$ is not cycic.

SOLUTION: As additive group, K es isomorfo a $(\mathbb{Z}/3\mathbb{Z} \times \overset{n)}{\cdots} \mathbb{Z}/3\mathbb{Z})$ which is not cyclic, since every element has order 3.

□