1. (1) Splitting field of $x^{p^n}-1$ over $GF(p)$

Notice that $x^{p^n}-1 = (x-1)^{p^n}$ so $x^{p^n}-1$ splits over $GF(p)$

i.e. $GF(p)$ itself is actually the splitting field.

(2) Splitting field of x^6+2x^3+2 over $GF(3)$

Notice that $\underline{x^6+2x^3+2 = (x^2+2x+2)^3}$

Rmk. this is not tricky, this is Frobenius automorphism.

and x^2+2x+2 is irreducible over $GF(3)$ (by check the root)

and degree 2 extension over char $=3 \neq 2$ is Galois

or you can check if α is root of x^2+2x+2 then $GF(3)(\alpha)$

is exact a splitting field. and it is separable.

so the splitting field is $GF(3)(\alpha) \cong GF(9)$

(3). Splitting field of x^4-2 over $\mathbb{Q}(i)$ and its Galois group

$$x^4-2 = (x^2-\sqrt{2})(x^2+\sqrt{2}) = (x+\sqrt[4]{2})(x-\sqrt[4]{2})(x+\sqrt[4]{2}i)(x-\sqrt[4]{2}i)$$

so the splitting field is $\mathbb{Q}(i, \sqrt[4]{2}) = K$, and $K/\mathbb{Q}$ also separable.

and since this is a galois extension

we know (we will know) $[\mathbb{Q}(i,\sqrt[4]{2}), \mathbb{Q}(i)] = |\underbrace{Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q}(i))}_{\text{denote by } G}|$

so the order of Galois group is 4

notice that $\sigma: K \longrightarrow K$

$\sqrt[4]{2} \longmapsto i\sqrt[4]{2}$ is of order 4

So $G \cong \mathbb{Z}/4\mathbb{Z}$

2. F field. K splitting field of $f(x)$ over F $\quad F \subset E \subset K$

pruf $\quad K$ splitting field of $f(x)$ over E

By definition. suppose the root set of $f(x)$ is

$\Omega = \{\alpha_1 \dots \alpha_n\}$

then $K = F(\Omega)$

Let K_1 be splitting field of $f(x)$ over E

then $K_1 = E(\Omega)$

Since $E \subset K$ it shows $K_1 = E(\Omega) \subset K(\Omega) = K$

and $F \subset E$ shows $K = F(\Omega) \subset E(\Omega) = K_1$

so $K = K_1$

3. K/F fin. normal extension. $F \subset E \subset K$

pruf. E/F normal iff E stable.

$(\Rightarrow)$ if E/F is normal, fin, extension

the by the definition E is a splitting field of a polynomial over F

Since $\forall\ \sigma \in \mathrm{Aut}_F K$, $\sigma|_F = id$

so $f^\sigma = f$

i.e. σ permutes the roots of all roots of f

But E has all root of $f \Rightarrow \sigma(E) = E$

$(\Leftarrow)$ if E/F is not normal, then there $\exists\ \alpha \in E$

s.t. $Irr(\alpha, F)$ has a root $\beta \in K \setminus E$

Let $\sigma: \alpha \mapsto \beta$ be the lift isomorphism of following diagram:

$$\begin{tikzcd} F(\alpha) \arrow[r, "\sigma"] & F(\beta) \\ F \arrow[u, dash] \arrow[r, "id"] & F \arrow[u, dash] \end{tikzcd}$$

the σ can extend to an element of $Aut_F K$ since

K is also a normal extension of $F(\alpha)$ and $F(\beta)$ (by HW. EX. 2)

$$\begin{tikzcd} K \arrow[r, "\tilde{\sigma}"] & K \\ F(\alpha) \arrow[u, dash] \arrow[r, "\sigma"] & F(\beta) \arrow[u, dash] \\ F \arrow[u, dash] \arrow[r, "id"] & F \arrow[u, dash] \end{tikzcd}$$

Now since $\beta \notin E$, $\tilde{\sigma}(E) \neq E$, contradiction.

4. Let $F \subset E \subset L$, $F \subset K \subset L$, $[L:F] < \infty$

prove if E/F, K/F normal. then $E \cap K/F$, EK/F normal.

$[L:F] < \infty$ shows $[E:F] < \infty$, $[K:F] < \infty$

i.e E/F, K/F are both finite normal extension

$\Rightarrow \exists\ f_1(x), f_2(x) \in F[x]$ such that

E, K are the splitting field of $f_1(x), f_2(x)$ over F respectively

Let L' be splitting field of $f_1(x)\cdot f_2(x)$ over F

then L' is also a finite normal extension of F

and $F \subset E \subset L'$, $F \subset K \subset L'$

$\forall\ \sigma \in Aut_F L'$, $\sigma(E) = E$, $\sigma(K) = K$

it implies $\sigma(E \cap K) = E \cap K$, $\sigma(EK) = EK$

since $F \subset E \cap K \subset L'$ $F \subset EK \subset L'$, $E \cap K$, EK stable

$\Rightarrow$ $E \cap K / F$ and EK/F normal.

5. as before. prove if K/F normal then EK/E normal.

$F \subset K \subset L$, $[L:F] < \infty$, K/F normal

$\Rightarrow$ K/F finite normal

$\Rightarrow$ $\exists\ f(x) \in F[x]$, K is the splitting field of $f(x)$ over F

$\Rightarrow$ suppose all roots of $f(x)$ form a set $\Omega = \{\alpha_1 \cdots \alpha_n\}$

$\Rightarrow$ $K = F(\alpha_1 \cdots \alpha_n)$

$\Rightarrow$ $EK = E(F(\alpha_1, \cdots \alpha_n))$, $F \subset E$ $\Rightarrow$ $EK = E(\alpha_1, \cdots \alpha_n)$

$\Rightarrow$ EK is the smallest field contains E and Ω

$\Rightarrow$ EK is the splitting field of $f(x)$ over E

$\Rightarrow$ $EK/_E$ is finite normal extension.

6. if K/E E/F normal is K/F normal ?

No

$$\begin{array}{ll} \mathbb{Q}(\sqrt[4]{2}) & \\ \quad | & \text{normal} \\ \mathbb{Q}(\sqrt{2}) & \\ \quad | & \text{normal} \\ \mathbb{Q} & \end{array}$$

not normal

7. Let $p_1 \dots p_m$ distinct primes. $K = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_m})$. show $Gal(K/\mathbb{Q})$

K is the splitting field of $f = (x^2 - p_1) \cdots (x^2 - p_m)$ over $\mathbb{Q}$

Since f is reducible with irreducible components $x^2 - p_i$

Consider the roots set $\Omega = \{\sqrt{p_1}, -\sqrt{p_1}, \dots, \sqrt{p_m}, -\sqrt{p_m}\}$

$Gal(K/\mathbb{Q})$ acts on Ω has m distinct orbits.

on which orbits the action is $\sigma_i : \sqrt{p_i} \longmapsto -\sqrt{p_i}$

So $Gal(K/\mathbb{Q}) = \underbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{m} = \mathbb{Z}_2^m$

(we will learn it)

Before exercise 8 we prove a lemma first.

Lemma: Sps. $\operatorname{char} F \neq 2$, $f(x)$ monic polynomial $\in F[x]$

$\deg f = n \geq 1$, and $f(x)$ has no repeated root.

Let E be the splitting field of $f(x)$ over F

$f(x) = (x - r_1) \cdots (x - r_n)$ $r_i \in E = F(r_1, \cdots r_n)$

$Gal(f) = Gal(E/F) \leq S_n$

Let $D = \prod_{1 \leq i < j \leq n} (r_i - r_j)$

then $\mathrm{Gal}(f) \subseteq A_n \iff D \in F$.

proof: $D = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ r_1 & r_2 & \cdots & r_n \\ \vdots & \vdots & & \\ r_1^{n-1} & r_2^{n-1} & \cdots & r_n^{n-1} \end{vmatrix}$

if σ odd, $\sigma(D) = -D$ if σ even $\sigma(D) = D$

i.e.

$$\begin{array}{ll} E & \mathrm{Gal}(E/E) \\ | & \\ F(D) & \mathrm{Gal}(E/F(D)) = \mathrm{Gal}(E/F) \cap A_n \\ | & \\ F & \mathrm{Gal}(E/F) \end{array}$$

8. $x^3 - 3x - 1$

proof: $D^2 = 81$, $D = \pm 9 \in \mathbb{Q} \Rightarrow F(D) = F \Rightarrow \mathrm{Gal}(E/F) = \mathrm{Gal}(E/F) \cap A_n$

i.e $\mathrm{Gal}(E/F) \leq A_n = A_3 = \mathbb{Z}_3$

only possibility is $\mathbb{Z}_3$ since

E/F is not trivial extension.

$$\begin{array}{cc} E & e \\ | & | \\ \mathbb{Q} & \mathbb{Z}_3 \end{array}$$

$x^3 - x - 1$

$D^2 = -23$, $D \notin \mathbb{Q}$

$\Rightarrow \mathrm{Gal}(E/\mathbb{Q}) = S_3$ subgroups: $\{e\}$, $\mathbb{Z}_3$, $\mathbb{Z}_2$, S_3.

Let $\underbrace{x_1 \quad x_2}_{\text{complex}}$ y be 3 roots.

real

$\sigma: x_1 \mapsto x_2 . \quad x_2 \mapsto x_1 \quad y \mapsto y$

$\beta: x_1 \mapsto x_2 \quad x_2 \mapsto y \quad y \mapsto x_1$

$$\begin{tikzcd}
 & \mathbb{Q}(x_1, y) \quad id & \\
\mathbb{Z}_2 \quad \mathbb{Q}(y) \arrow[ur, dash] & & \mathbb{Q}(x_1) \quad \mathbb{Z}_3 \arrow[ul, dash] \\
 & \mathbb{Q} \arrow[ul, dash] \arrow[ur, dash] & \\
 & S_3 &
\end{tikzcd}$$

9. Give all subgroups of $Gal(GF(p^n)/GF(p))$ and fixed field.

proof. Consider Frobenius automorphism.

$$Frob_p(GF(p)) = GF(p)$$

$$\Rightarrow Frob_p \in Gal(GF(p^n)/GF(p))$$

$$\langle Frob_p \rangle = \mathbb{Z}_n$$

$$|\langle Frob_p \rangle| = n = [GF(p^n) : GF(p)] \geq |Gal(GF(p^n)/GF(p))|$$

$$\Rightarrow \langle Frob_p \rangle = Gal(GF(p^n)/GF(p)) = \mathbb{Z}/n\mathbb{Z}$$

for any positive factor of n, denoted by d.

$\langle Frob_p^d \rangle$ is the only subgroup of order n/d

the fixed field is F_{p^d}

10. p odd prime number. K splitting field of $x^{p^n}-1$ over $\mathbb{Q}$

(1). prove $[K:\mathbb{Q}] = p^{n-1}(p-1)$

Let ζ be primitive root of unit of order p^n

Let $f(x) = Irr(\zeta, \mathbb{Q})$

We prove $f(x) = \prod (x - \zeta^i)$, $(i, p) = 1$ and $1 \le i \le p^n$

Claim. for any prime number $q \ne p$. ζ^q is zero point of $f(x)$

if not. suppose $Irr(\zeta^q, \mathbb{Q}) = g(x)$

then $(f(x), g(x)) = 1$,

but $f(x) \mid x^{p^n} - 1$, $g(x) \mid x^{p^n} - 1 \Rightarrow f(x) g(x) \mid x^{p^n} - 1$

i.e $\exists\ t(x) \in \mathbb{Q}[x]$ s.t $x^{p^n} - 1 = f(x) g(x) t(x)$

$\Rightarrow$ $f(x), g(x), t(x)$ monic, integer coefficient.

$x^{p^n} - \bar{1} = \bar{f}\ \bar{g}\ \bar{t}$ mod q since $(p, q) = 1$

$x^{p^n} - \bar{1}$ has no repeated factor.

$\Rightarrow (\bar{f}(x), \bar{g}(x)) = 1$

But $g(\zeta^q) = 0$ is ζ is zero point of $g(x^q)$

$\Rightarrow f(x) \mid g(x^q)$

$\Rightarrow \bar{f} \mid \bar{g}(x^q) = (\bar{g}(x))^q$ 与 $(\bar{f}, \bar{g}) = 1$

For any $1 \le i \le p^n$, $(i, p) = 1$ Let $i = q_1 \cdots q_s$

then $q_j \ne p$ $j = 1, \ldots, s$

$\Rightarrow \zeta^i$ is zero point of $f(x)$ $\Rightarrow \prod(x-\zeta^i) \mid f(x)$

On the other hand

since ζ is not a zero point of x^m-1 $(1 \le m < p^n)$

$\Rightarrow \left(f(x), x^m-1\right) = 1$

So the zero point of $x^{p^n}-1$ is all primitive roots of unit of order p^n

(2). $Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$ and $\mathbb{Z}_{p^n}$ is cyclic generated by primitive root mod p^n.