1. Find $\mathrm{Irr}(\alpha, F)$

(1). $\alpha = \sqrt{2}+\sqrt{3}$, $F = \mathbb{Q}(\sqrt{6})$

note that $\alpha^2 = 5+2\sqrt{6} \in \mathbb{Q}(\sqrt{6})$

find $f(x) = x^2 - (5+2\sqrt{6})$.

Only need to show $f(x)$ is irreducible in $\mathbb{Q}(\sqrt{6})[x]$.

If $f(x)$ is reducible, then $\alpha \in F$

since $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$, $[\mathbb{Q}(\sqrt{6}):\mathbb{Q}] = 2$. this is impossible

Hence $f(x)$ is irreducible.

i.e. $\mathrm{Irr}(\alpha, F) = x^2 - (5+2\sqrt{6})$

(2). $\alpha = \sqrt{2}+\sqrt{3}$. $F = \mathbb{Q}(\sqrt{2})$

note that $(\alpha - \sqrt{2})^2 = 3$

so find $f(x) = (x-\sqrt{2})^2 - 3 = x^2 - 2\sqrt{2}x - 1$

(3). $\alpha = \sqrt{2}+\sqrt{3}$. $F = \mathbb{Q}$

note that

$$(\alpha - \sqrt{2})^2 = 3 \Rightarrow \alpha^2 - 1 = 2\sqrt{2}\alpha$$

$$\Rightarrow (\alpha^2-1)^2 = 8\alpha^2$$

$$\Rightarrow \alpha^4 - 10\alpha^2 + 1 = 0$$

find $f(x) = x^4 - 10x^2 + 1$, only need to prove

$f(x)$ is irreducible in $\mathbb{Q}[x]$

you can show it by set the coefficients such as

sps $f(x) = (x^2+ax+b)(x^2+cx+d)$ and get a contradiction.

I give another method by Eisenstein criterion:

$f(x)$ irre. iff $\underbrace{f(x+1)}$ irre iff $g(2x)$ irre
denote: $g(x)$

set $g(2x) = 16x^4+32x^3-16x^2+32x-8 = 8h(x)$

where $h(x) = 2x^4+4x^3-2x^2+4x-1$

$h(x)$ irre iff $\widetilde{h(x)} = x^4 \cdot h(\frac{1}{x}) = -x^4+4x^3-2x^2+4x+2$ irre.

take 2. by Eisenseein Criterion, $\widetilde{h(x)}$ irre. done.

2. Let $K/F$ be extension

(1). Let $a \in K$. if $a \in F(a^m)$ where $m>1$. Prove $a$ is alg.

$a \in F(a^m)$, i.e. $\exists f(x), g(x) \in F[x]$ s.t

$$a = \frac{f(a^m)}{g(a^m)}$$

the set $h(x) = x g(x^m) - f(x^m) \in F[x]$, $h(a)=0$

we only need to show $h(x) \neq 0$, Let $\deg g = s$, $\deg f = t$

since $m>1$. $\deg x \cdot g(x^m) = 1+ms$ $\deg f(x^m) = mt$

$\Rightarrow \quad mt \neq ms+1$

( think about $m(t-s)=1$ . it forces $m, t-s \in \{\pm 1\}$ )

$\Rightarrow \deg h(x) > 0 \quad \Rightarrow h(x) \neq 0$

(2). If $a \in K$, $a$ alg. of odd degree. Prove $F(a) = F(a^2)$.

Obviously, $a^2 = a \cdot a$ shows $F(a^2) \subseteq F(a)$.

Now since $a$ alg. of odd degree.

Set $Irr(a, F) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$, $n$ odd and $b_i \in F$

$\Rightarrow \quad a^n + b_{n-2}a^{n-2} + \cdots + b_1 a = b_{n-1}a^{n-1} + \cdots + b_0$

$\Rightarrow \quad a(a^{n-1} + b_{n-2}a^{n-3} + \cdots + b_1) = b_{n-1}a^{n-1} + \cdots + b_0$

since $\deg Irr(a, F) = n$, $n-1 < n \Rightarrow a^{n-1} + b_{n-2}a^{n-3} + \cdots + b_1 \neq 0$

$\Rightarrow \quad a = \dfrac{b_{n-1}a^{n-1} + \cdots + b_0}{a^{n-1} + b_{n-2}a^{n-3} + \cdots + b_1}$

↑ all power of $a$ here are even.

i.e $a \in F(a^2)$ i.e $F(a) \subseteq F(a^2)$

$\Rightarrow F(a) = F(a^2)$.

3. Let $u$ be a root of $x^3-6x^2+9x+3$

(1). Prove $[\mathbb{Q}(u):\mathbb{Q}]=3$

Let $f(x)=x^3-6x^2+9x+3$, take $p=3$, by Eisenstein criterion

$f(x)$ is irr. So $[\mathbb{Q}(u):\mathbb{Q}]=\deg f=3$

(2). Represent $u^4$ $(u+1)^{-1}$, $(u^2-6u+8)^{-1}$ as $\mathbb{Q}$-linear combination of $\{1, u, u^2\}$.

$$u^4 = u^3\cdot u = (6u^2-9u-3)\cdot u$$
$$= 6u^3-9u^2-3u$$
$$= 6(6u^2-9u-3)-9u^2-3u$$
$$= 36u^2-54u-18-9u^2-3u$$
$$= 27u^2-57u-18.$$

$$\begin{array}{r|l} x+1 & x^2-7x+16 \\ \hline & x^3-6x^2+9x+3 \\ & x^3+x^2 \\ \hline & -7x^2+9x \\ & -7x^2-7x \\ \hline & 16x+3 \\ & 16x+16 \\ \hline & -13 \end{array}$$

i.e. $x^3-6x^2+9x+3=(x+1)(x^2-7x+16)-13$

i.e $(u+1)(u^2-7u+16)=13$

i.e $(u+1)^{-1}=\frac{1}{13}(u^2-7u+16)$

$f$ $g$

$x$ $\quad x^3-6x^2+9x+3 \quad x^2-6x+8 \quad x-9$

$x^3-6x^2+8x$

$x+3$

$x^2+3x$

$-9x+8$

$-9x-27$

$35$

i.e. $f = xg + x+3$

$g = (x-9)(x+3) + 35$

$g = (x-9)(f-xg) + 35$

$g = (x-9)f - (x-9)xg + 35$

$\Rightarrow (x^2-9x+1)g - (x-9)f = 35$

take $u$. $(u^2-9u+1)g(u) = 35$

$\Rightarrow (g(u))^{-1} = \frac{1}{35}(u^2-9u+1)$

4. Let $k$ be a field. if $x^n-a \in k[x]$ irr.

pre: for any possitive factor $m$ of $n$

$x^m-a$ also irr. in $k[x]$.

Since $x^n-a$ irr. $\exists\ u$ s.t.

$k(u) \simeq k[x]/(x^n-a)$, $u^n-a=0$ in $k(u)$.

and $[k(u):k] = n$ if $dm = n$, $d \geq 1$. $d \in \mathbb{Z}$

then $(u^d)^m - a = u^{dm} - a = u^n - a = 0$.

if $x^m - a$ not irr in $k[x]$

then since $(u^d)^m - a = u^n - a = 0$

we have $[k(u^d):k] < \deg(x^m - a) = m$

so $[k(u):k(u^d)] > \frac{n}{m} = d$

but consider $g(x) = x^d - u^d$ over $k(u^d)$

$g(u) = 0$ shows

$[k(u):k(u^d)] \leq \deg(x^d - u^d) = d$ Contradiction.

5. $k$ fld. $x$ transcendental over $k$ $u \in k(x)$, $u \notin k$

Prove $x$ is alg. over $k(u)$.

$x$ trans. shows $k(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in k[x] \text{ and } g(x) \neq 0 \right\}$.

so $\exists$ $f, g$ s.t $u = \frac{f(x)}{g(x)}$

and $u \notin k$ shows $\deg f \neq \deg g$. and $\deg f^2 + \deg g^2 > 0$.

so take $F(y) = ug(y) - f(y)$ in $k(u)[y]$

then $F(x) = 0$ and $\deg F(y) = \max\{\deg f, \deg g\} > 0$

i.e $x$ is algebraic over $k(u)$.

6. prove $Aut(\mathbb{R}) = \{id\}$.

Sps $\sigma \in Aut(\mathbb{R})$

$\forall\ x \in \mathbb{R}_{>0}$, $\exists \sqrt{x} \in \mathbb{R}$

so $\sigma(x) = \sigma((\sqrt{x})^2) = (\sigma(\sqrt{x}))^2 > 0$

so $\sigma$ preserve positivity of numbers.

so if $y - z > 0$ $\sigma(y-z) > 0 \Rightarrow \sigma(y) - \sigma(z) > 0$

so $\sigma$ preserve order.

Now suppose $\beta \in \mathbb{R}$, an arbitrary real number.

use the trick as Dedekind. Cut.

Define $S = \{a \in \mathbb{Q} \mid a < \beta\}$ and $S' = \{b \in \mathbb{Q} \mid b \geq \beta\}$

the $\beta$ is the unique real number satisfying.

$$a < \beta \leq b, \quad \forall\ a \in S,\ b \in S'$$

But 1°. $\sigma$ fixes all rational number

Since $\sigma(1) = 1$, $\sigma(m) = m\sigma(1) = m$

$$\Rightarrow \sigma\left(\frac{p}{q}\right) = \sigma(p)\,\sigma(q^{-1}) = \sigma(p)(\sigma(q))^{-1} = \frac{p}{q}$$

2° $\sigma$ preserve order

So $\sigma$ fixes $\beta$, i.e $\sigma(\beta) = \beta$, $\forall\ \beta \in \mathbb{R}$. $\Rightarrow \sigma = id$.

it shows $Aut(\mathbb{R}) = \{id\}$

7. Let $L/F$ field extension $E, K$ two intermediate field.

pure.

(1). $[EK:F]$ finite iff $[E:F], [K:F]$ finite.

($\Rightarrow$) $[EK:F]$ finite.

$[EK:F] = [EK:E][E:F] = [EK:K][K:F] < \infty$

$\Rightarrow$ $[E:F]$ and $[K:F]$ finite.

($\Leftarrow$) only need to show

(2). $[EK:F] \leq [E:F][K:F]$

WLOG sps $[E:F]$, $[K:F]$ finite since if one of them is infinite the this inequality is undefined.

Now we can set $[E:F]=n$, $[K:F]=m$

$E = F(\alpha_1 \cdots \alpha_n)$, $K = F(\beta_1 \cdots \beta_m)$

with $F$-basis $\{\alpha_1, \cdots \alpha_n\}$ and $\{\beta_1 \cdots \beta_m\}$

then $EK = F(\alpha_1 \cdots \alpha_n, \beta_1 \cdots \beta_m) = E(\beta_1 \cdots \beta_m)$

i.e. $\beta_1 \cdots \beta_m$ span $EK$ over $E$

i.e. $[EK:E] \leq m$

hence $[EK:F] = [EK:E][E:F] \leq mn = [E:F][K:F]$

Therefore. $[EK:F] < \infty$

(3). If $([E:F], [K:F]) = 1$, then $[EK:F] = [E:F][K:F]$

we have $n \mid [E_K : F]$, $m \mid [E_K : F]$

Since $(m,n) = 1 \Rightarrow mn \mid [E_K : F]$

But $[E_K : F] \le mn$. it forces $[E_K : F] = mn$.

8. Construct a finite field with 8 eles and write the table.

notice that $f(x) = x^3 + x + 1$ is irre. in $GF(2)[x]$

so $GF(2)[x]/(f(x))$ is a field with 8 eles.

denote the root of $f(x)$ by $u$.

then $GF(2)(u) = \{ a + bu + cu^2 \mid a, b, c \in GF(2) \}$.

with addition:

$$(a_1 + b_1 u + c_1 u^2) + (a_2 + b_2 u + c_2 u^2) = (a_1 + a_2) + (b_1 + b_2)u + (c_1 + c_2)u^2$$

multiplication:

$$(a_1 + b_1 u + c_1 u^2)(a_2 + b_2 u + c_2 u^2)$$

$$= a_1 a_2 + (b_1 a_2 + b_2 a_1)u + (c_1 a_2 + c_2 a_1 + b_1 b_2)u^2$$

$$+ (b_1 c_2 + c_1 b_2)\underline{u^3} + c_1 c_2 \underline{u^4}$$

but as $u^3 + u + 1 = 0$ $\quad \underline{u^3} = -u - 1 = u + 1$

$\underline{u^4} = u(u^3) = u^2 + u$.

9. Let $f(x)=x^2+1$ $g(x)=x^2-x-1$

(1). Prove $f, g$ irred in $GF(3)[x]$

$GF(3)=\{0,1,-1\}$

$f(0), f(1), f(-1)\neq 0$ $g(0), g(1), g(-1)\neq 0$

So $f, g$ irre.

(2). Let $\alpha, \beta$ denote roots of $f, g$ in $GF(9)$

give an iso of $GF(3)(\alpha)$ to $GF(3)(\beta)$.

Since $f(\beta+1)=(\beta+1)^2+1=\beta^2+2\beta+2=\beta^2-\beta-1=g(\beta)=0$

So $\sigma: GF(3)(\alpha) \xrightarrow{\sim} GF(3)(\beta)$

$\alpha \longmapsto \beta+1$

and check $\sigma$ is iso.

10. (1). Prove $GF(p^m)\subseteq GF(p^n)$ iff $m|n$.

Regard $GF(p^m)$ as roots of $x^{p^m}-x \in GF(p)[x]$

($\Rightarrow$) $GF(p^m)\subseteq GF(p^n) \Rightarrow [GF(p^n):GF(p)]=[GF(p^n):GF(p^m)]$
$[GF(p^m):GF(p)]$

$\Rightarrow m|n$

($\Leftarrow$) $m|n \Rightarrow x^{p^m}-x \mid x^{p^n}-x \Rightarrow GF(p^m)\subseteq GF(p^n)$.

(2). In $GF(p)[x]$ prove $x^{p^m}-x \mid x^{p^n}-x$ iff $m|n$

Corollary of (1).