HW09

(1)

SOLUTION.

Let $f(x)$ denote the polynomial in question.

(a) Irreducible: $f(x)$ doesn't have a linear factor in $\mathbb{F}_2[x]$ since $f(1) \not\equiv 0 \mod 2$.

(b) Reducible: $f(1) \equiv 0 \mod 3$. Use polynomial division to compute $f(x)/(x-1) = x^2+x-1 =: g(x)$. Since $g(1), g(2) \not\equiv 0 \mod 3$, $g(x)$ is irreducible. Therefore $f(x) = (x-1)(x^2+x-1)$.

(c) $x^4-4 = (x^2+2)(x^2-2)$; 2,3 are not squares mod 5, so these quadratic factors are irreducible.

(d) Let $y = x^2$; then $f(x) = y^2 + 10y + 1$. We can use the quadratic equation to compute the roots, and see that they are not integers (or even rational numbers).

(e) $f(x)$ is Eisenstein at $p = 3$, and is therefore irreducible.

(f) Same as above.

(2)

SOLUTION.

(a) Since $\mathbb{Q}(2+\sqrt{3}) = \mathbb{Q}(\sqrt{3})$, the degree of the extension over $\mathbb{Q}$ is 2.

(b) Let $\alpha = \sqrt[3]{2}$; then the element is $1+\alpha+\alpha^2$, which is in $\mathbb{Q}(\alpha)$. The degree of α is 3. The degree of $1+\alpha+\alpha$ is therefore a factor of 3. Since it's not in $\mathbb{Q}$, the degree is 3.

(c) Let $\alpha = \sqrt{3+2\sqrt{2}}$. Then $\alpha^2 = 3+2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, which has degree 2 over $\mathbb{Q}$. Check that indeed, $\deg_{\mathbb{Q}}(\alpha) = 4$ (because $\alpha \notin \mathbb{Q}(\sqrt{2})$).

(d) Use the same kinds of calculations in the previous part; conclude that $\deg_{\mathbb{Q}}(\alpha) = 4$.

(3)

SOLUTION.

If $\alpha_i^2 \in \mathbb{Q}$ for every i, then the degree of the extension $F/\mathbb{Q}$ is a power of 2, say 2^k. If $\sqrt[3]{2} \in F$, $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset F$, so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ must divide 2^k. But $\deg_{\mathbb{Q}}(\sqrt[3]{2}) = 3$.

(4)

SOLUTION.

It's clear that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Compute the powers of α to obtain linear combinations of powers of α equal to $\sqrt{2}$ and $\sqrt{3}$, proving the reverse inclusion. (See scratchwork for how I thought about it.)

The degree of $\sqrt{2}$ over $\mathbb{Q}$ is 2, and the degree of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ is also 2 (since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, the degree is more than 1), the total degree is 4.

The minimal polynomial is $m_{\alpha,\mathbb{Q}}(x) = x^4 - 10x^2 + 1$.

Calculations:

$\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ so $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$\alpha^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6} \implies \alpha^2 - 5 = 2\sqrt{6}$

$\implies (\alpha^2 - 5)^2 = 4 \cdot 6 = 24.$

$\alpha^4 - 10\alpha^2 + 25 = 24$

$\underbrace{\alpha^4 - 10\alpha^2 + 1}_{\text{minimal polyn.}} = 0$

$\frac{1}{2}\alpha(\alpha^2 - 5) = (\sqrt{2} + \sqrt{3})\sqrt{6} = 2\sqrt{3} + 3\sqrt{2}$

$\implies \frac{1}{2}\alpha(\alpha^2 - 5) - 2\alpha = \sqrt{2}$ and $\frac{1}{2}\alpha(\alpha^2 - 5) - 3\alpha = -\sqrt{3}$

$\implies \sqrt{2}, \sqrt{3} \in \mathbb{Q}(\alpha). \implies \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha). \implies \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$,

so $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ ↑ $x^2 - 2$

↑ $x^2 - 3$

(5)

(a) $x^4-2=0 \rightsquigarrow x^4=2$. Let $\alpha=\sqrt[4]{2}$.

$(x^2+\sqrt{2})(x^2-\sqrt{2})=0$ roots: $\pm i\alpha, \pm\alpha$. are generated by $i\alpha$.

Splitting field: $\mathbb{Q}(i\alpha,\alpha)=\mathbb{Q}(i,\alpha)$

$\deg_{\mathbb{Q}}(\alpha)=4$ since x^4-2 is Eisenstein @ $p=2$ and thus irreducible.

$i \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$, so $[\mathbb{Q}(i,\alpha):\mathbb{Q}(\alpha)]=2$ $(m_{i,\mathbb{Q}(\alpha)}(x)=x^2+1)$

$\Rightarrow [\mathbb{Q}(i,\alpha):\mathbb{Q}]=8$.

(b) x^4+2 is also Eisenstein at $p=2$ and is irreducible.

Let $\alpha=\sqrt[4]{2}$, ζ = a primitive 8^{th} root of unity. (4^{th} root of -1)

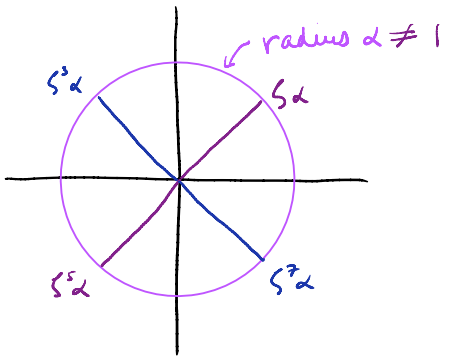
The 4 roots are $\zeta\alpha, \zeta^3\alpha, \zeta^5\alpha, \zeta^7\alpha$. $=\pm\zeta\alpha, \pm\zeta^3\alpha$.

Note $\zeta^3\alpha/\zeta\alpha=\zeta^2=i \in$ splt. field $=\mathbb{Q}(\zeta\alpha,\zeta^3\alpha)$

So $\mathbb{Q}(\zeta\alpha,\zeta^3\alpha)=\mathbb{Q}(\zeta\alpha,i)$.

Also, $i \notin \mathbb{Q}(\zeta\alpha)$. ← length considerations.

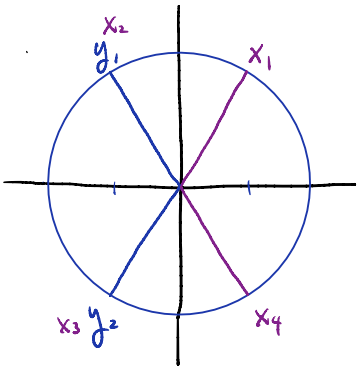
$\Rightarrow [\mathbb{Q}(\zeta\alpha,i):\mathbb{Q}]=8$.



(c) $f(x) = x^4 + x^2 + 1$

$y = x^2 \rightsquigarrow f(x) = y^2 + y + 1$

$$y = \frac{-1 \pm \sqrt{1-4}}{2} = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$$



roots of $f(x)$: $\pm\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$.

note: $\frac{1}{2} + i\frac{\sqrt{3}}{2} = x_1 = e^{i\frac{\pi}{3}}$.

Splitting field: $\mathbb{Q}(e^{i\frac{\pi}{3}})$ since all other roots are powers of $e^{i\frac{\pi}{3}}$.

note: $\mathbb{Q}(\frac{1}{2} + i\frac{\sqrt{3}}{2}) = \mathbb{Q}(i\sqrt{3}) = \mathbb{Q}(\sqrt{-3})$

↖ root of $x^2 + 3$.

$\Rightarrow [\mathbb{Q}(e^{i\frac{\pi}{3}}) : \mathbb{Q}] = 2$.

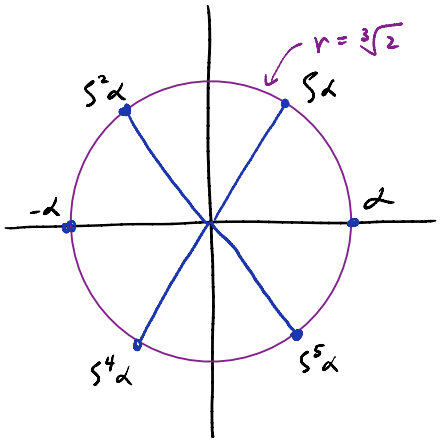
(d) $f(x) = x^6 - 4 = (x^3 + 2)(x^3 - 2)$

Let $\alpha = \sqrt[3]{2}$, $\zeta = \zeta_6$.

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

Since $\zeta = \zeta\alpha/\alpha \in$ split field,

the splitting field $= \mathbb{Q}(\zeta, \alpha)$.



$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, and $\deg_{\mathbb{Q}(\alpha)}(\zeta) = 3 \Rightarrow [\mathbb{Q}(\zeta, \alpha) : \mathbb{Q}] = 9$.

⑥ prime p, $a \in \mathbb{F}_p^\times$

$f(x) = x^p - x + a$

Separable:

If α is a root, then

$$(\alpha+1)^p - (\alpha+1) + a$$

$$= \alpha^p + 1 - (\alpha+1) + a$$

$$= \alpha^p - \alpha + a = 0.$$

Since any $K/\mathbb{F}_p$ has $\mathbb{F}_p$ has the prime subfield. ($\operatorname{char} K = p$)

$\{\alpha, \alpha+1, \dots, \alpha+(p-1)\}$ are all distinct, and are all roots.

There are p of these, so these are the roots of $f(x)$.

$\Rightarrow f(x)$ is separable.

Irreducible:

Let $b \in \mathbb{F}_p$. $\Rightarrow b^{p-1} = 1$

Then $f(b) = b^p - b + a = b - b + a = a \neq 0$.

$\Rightarrow f$ has no roots in $\mathbb{F}_p$

$\Rightarrow f$ is irreducible (since any root α of f must have degree a power of p).

⑦ $f(x) \in \mathbb{F}_p(x)$

The multinomial coefficients are all multiples of p, except the pure terms.

(Can use binomial coefficients + induct:

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

$f(x)^p = (a_n x^n)^p + (a_{n-1} x^{n-1} + \cdots + a_1 x + a_0)^p$)